NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

AN EVALUATION METHODOLOGY FOR THE USABILITY AND SECURITY OF CLOUD-BASED FILE SHARING TECHNOLOGIES

by

Trek C. Potter

September 2012

Thesis Advisor:	Alan Shaffer
Thesis Co-Advisor:	Simson Garfinkel
Second Reader:	William Welch

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** September 2012	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE An Evaluation Methodology for the Usability and Security of Cloud-based File Sharing Technologies		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Trek C. Potter			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number _____N/A_____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE** A	

13. ABSTRACT (maximum 200 words)

To operate effectively and maintain national security, the DoD relies on the ability to ensure authorized access to information, while protecting that information from unauthorized users. Non-malicious insider threats involving information leakage typically receive little attention, though their impact is significant. This thesis focuses on how the act of file sharing contributes to non-malicious insider threats. Current file sharing methods provide neither the usability users require nor the security the organization requires. Security without usability results in users bypassing securing features, and systems that are usable but not secure are invariably compromised. Therefore, usability and security must be properly aligned to attain true security. Cloud-based file sharing technologies provide promising alternatives for both usable and secure file sharing. As the federal government moves toward the cloud, new programs assess the back-end security of commercially available cloud-based technologies. Building on prior research, this thesis develops a methodology for evaluating the usability and security of cloud-based file sharing technologies from the end-user perspective. This methodology adapts and combines the concepts of heuristics evaluation and cognitive walkthrough. Specifically, the heuristics evaluation assesses whether a cloud-based file sharing technology implements critical usability and security principles, and the cognitive walkthrough determines how usably the principles are implemented. The thesis concludes with a demonstration of how the methodology is conducted. The results of this methodology will assist organizations in properly assessing a technology for official use by DoD.

14. SUBJECT TERMS Cloud Computing, File Sharing, Insider Threat, Information Assurance, Usability, HCI, HCI-SEC, Human Factors			**15. NUMBER OF PAGES** 111
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

AN EVALUATION METHODOLOGY FOR THE USABLILITY AND SECURITY OF CLOUD-BASED FILE SHARING TECHNOLOGIES

Trek C. Potter
Captain, United States Air Force
B.S., Weber State University, 2007

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
September 2012

Author: Trek C. Potter

Approved by: Alan Shaffer
Thesis Advisor

Simson Garfinkel
Thesis Co-Advisor

William Welch
Second Reader

Dan Boger
Chair, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

To operate effectively and maintain national security, the DoD relies on the ability to ensure authorized access to information, while protecting that information from unauthorized users. Non-malicious insider threats involving information leakage typically receive little attention, though their impact is significant. This thesis focuses on how the act of file sharing contributes to non-malicious insider threats. Current file sharing methods provide neither the usability users require nor the security the organization requires. Security without usability results in users bypassing securing features, and systems that are usable but not secure are invariably compromised. Therefore, usability and security must be properly aligned to attain true security. Cloud-based file sharing technologies provide promising alternatives for both usable and secure file sharing. As the federal government moves toward the cloud, new programs assess the back-end security of commercially available cloud-based technologies. Building on prior research, this thesis develops a methodology for evaluating the usability and security of cloud-based file sharing technologies from the end-user perspective. This methodology adapts and combines the concepts of heuristics evaluation and cognitive walkthrough. Specifically, the heuristics evaluation assesses whether a cloud-based file sharing technology implements critical usability and security principles, and the cognitive walkthrough determines how usably the principles are implemented. The thesis concludes with a demonstration of how the methodology is conducted. The results of this methodology will assist organizations in properly assessing a technology for official use by DoD.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

CNSS	Committee on National Security Systems
CERT	Computer Emergency Response Team
CSP	Cloud Service Provider
DAC	Discretionary Access Control
DoD	Department of Defense
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
FedRAMP	Federal Risk and Authorization Management Program
FISMA	Federal Information Security Management Act
FTP	File Transfer Protocol
GSA	General Services Administration
HCI	Human Computer Interaction
HCI-SEC	Human Computer Interaction and Security
IA	Information Assurance
IEEE	Institute of Electrical and Electronics Engineers
IT	Information Technology
ITS	Insider Threat Study
ISO	International Organization for Standardization
LAN	Local Area Network
NIST	National Institute of Standards and Technology
NCOIC	Non-Commissioned Officer in Charge
NSTAC	National Security Telecommunications Advisory Committee
OS	Operating System
PII	Personally Identifiable Information
PGP	Pretty Good Privacy
PKI	Public Key Infrastructure
SP	Special Publication
SAML	Security Assertion Markup Language
SAN	Storage Area Network
SEI	Software Engineering Institute

SME	Subject Matter Expert
SOUP	Symposium on Usable Privacy and Security
SSAE	Statements on Standards for Attestation Engagements
SSL	Secure Sockets Layer
SSO	Single Sign On
U.S.	United States
USB	Universal Serial Bus
UI	User Interface

ACKNOWLEDGMENTS

I would like to thank my outstanding thesis committee: Alan Shaffer, Simson Garfinkel, and Joe Welch. I am sincerely grateful for the time and attention they've devoted to my work over the last year. Without their experience, wisdom, and insightful direction, this thesis would not have been possible.

With all my heart, I am grateful for my family. My dear wife, Dani, and my loving children have patiently supported me through the many hours I've spent away from them while completing my research. I truly appreciate their prayers, thoughts, and encouragement.

Finally, I give thanks to God for supporting me with strength, purpose, and encouragement through all the challenges while accomplishing this research.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PROBLEM, PURPOSE AND METHODS

The ability for an organization's employees to share information and collaborate in its production is of critical importance. Particularly in the military, success on the battlefield depends on the ability to share information, yet the current file sharing capabilities afforded to Department of Defense (DoD) employees are either not secure, not usable, or neither secure nor usable. This lack of usable security exacerbates the non-malicious insider threat to DoD information systems. As a consequence, unintended data breaches resulting from this threat degrade the security posture of DoD networks.

This thesis seeks to understand how the lack of usability with the DoD's currently approved file sharing security measures and policies leads to increased residual security risk for DoD information systems. This thesis examines current DoD IA policies to show options available to employees (i.e., insiders) to securely store and share files, and shows these policies are cumbersome and difficult to follow. Legacy methods are used, including e-mail and removable media (thumb drives, disks, etc.), but they are not secure and do not scale. On an enterprise level, e.g., within the DoD, sharing solutions exist that incorporate Microsoft SharePoint or shared drives on a Storage Area Network (SAN), but they have profound problems in terms of interoperability, usability, and deployability. Cloud-based file storage and sharing solutions have developed over the past few years into what promises to be a possible replacement for legacy file sharing mechanisms. Still, it is uncertain whether cloud-based solutions can meet the security and scalability requirements for the DoD.

The ultimate purpose of this thesis is to evaluate solutions that bridge the gap between usability and security in a way that will create a truly secure solution for DoD employees. As file-sharing requirements are not unique to DoD, the concepts found in this thesis may apply generally to other sectors of society.

To achieve its purpose, this thesis develops an evaluation methodology for assessing the usability and security of cloud-based file sharing technologies. This

methodology includes a heuristics evaluation, based on numerous usability and security principles needed for secure file sharing, and a cognitive walkthrough of the most promising of the alternatives. Finally, a demonstration of this methodology shows how the methodology can be applied in order to find a solution capable of filling an organization's needs.

B. UNDERSTANDING THE THREAT

DoD information technology (IT) security professionals are the defenders of critical defense-related systems, positioned on a virtual perimeter and waging a battle both to protect and to provide access to an organization's information. They must fully understand and anticipate both external and internal threats to their IT systems. An "outsider" in the cyber context is defined generally as an individual who has not been granted authorized access to an organization's information systems. Enemy outsiders will attempt to exploit an information system without authorized access, i.e., by working around or overcoming existing security measures. Conversely, "insiders" have been granted some level of authorized access to an organization's information systems. The threats posed from insiders can be broken down into two categories: malicious and non-malicious. Malicious insiders intentionally exploit an information system to harm the organization for personal gain, e.g., financial or political. Non-malicious insiders, on the other hand, are those with authorized access to information who harm the information system without any intention of causing damage to the organization or its systems.

Much research has been dedicated to understanding the "who, what, and why" of cyber threats. But the focus of research with respect to these types of insider threats has been unbalanced. Outsider and malicious insider threats have received the majority of security research focus, while far less research has been done to understand and address the actions of the non-malicious insider, often perceived as less significant. One researcher attributes this lack of alarm to the human tribal instinct, where organizations want to believe that their own members can be trusted (Lynch, 2006). Overlooking the threat of non-malicious insiders can be detrimental. Most analyses of data breaches indicate that the majority originates with non-malicious insiders. For example, the

Privacy Rights Clearinghouse indicated that 87% of all data loss resulting from insider actions was attributable to non-malicious insiders (Privacy Rights Clearinghouse, 2011). Other studies have reported that data loss due to negligent insiders account for 40–70% of all data breaches (Lynch, 2006).

The costs associated with non-malicious data breaches are especially high (Cisco, 2008). Foremost among these are external costs to the individual or organization if the leaked information is intercepted and exploited by an outside adversary. Fortunately, this consequence is not always certain, as information leaked does not always make it into malicious hands. However, there are internal costs associated with information breaches, such as the significant administrative costs in time and money to find and repair a vulnerability created by the breach. As well, when PII is leaked there are time costs in contacting victims of the breach, as well as money costs in providing identity theft remediation. When sensitive information is leaked, there are productivity costs when network accounts must be shut down and protected or scrubbed, computers must be seized, and users are unable to conduct operations for a period of time. These external and internal costs can lead to a reputational cost for the organization as well.

C. NON-MALICIOUS INSIDER MOTIVATION

In light of these assertions, cyber defenders are likely to ask themselves why so many well-intentioned employees are causing such damage to their organizations. The explanation is the organization's failure to align usability and security. The potential for real damage, or the inadvertent creation of a new vulnerability, exists every time a well-intentioned user must circumvent an organization's security policies to get work done. Understanding why non-malicious insiders choose to circumvent security is the key to stopping such bad behavior.

Though they may not understand the severity of the threat, most organizations, including the DoD, recognize that non-malicious insiders pose some level of risk. Thus, organizations try to attack the problem with stronger security policies, such as more robust user training, auditing, and forcing users to adopt longer passwords. Such policies are meant to prevent users' bad actions before they happen, and auditing is intended to

catch bad behaviors after the fact. However, even with these countermeasures in place, the non-malicious insider threat continues to cause significant data breaches. These countermeasures are ineffective as they treat only the symptoms of the problem by addressing the individual actions that result in such behavior. They do not mitigate the cause of the threat, i.e., the circumstances that lead non-malicious insiders to circumvent security in the first place. If we can identify and eliminate these circumstantial factors, we can reduce their occurrence.

Numerous psychological and human factors drive non-malicious insiders to circumvent security measures; however, this study will focus on technology rather than psychology. On a technological level, one predominant motivator for security control circumvention stands out among the rest: when security mechanisms are too difficult for employees to use. If following a particular security measure makes it significantly harder for an employee to do his or her job, the chances are far greater that the employee will choose not to follow or abide by the measure.

D. THE THREAT OF UNUSABLE SECURITY

The idea that security mechanisms can be difficult to follow is not a new concept. There is a popular belief among users of technology that the terms "usability" and "security" are opposing forces that must be balanced. Usability refers generally to "the extent to which the users of products are able to work effectively, efficiently and with satisfaction" (International Organization for Standardization [ISO], 1998). Alternately, information security, known as information assurance (IA) by DoD, refers to "measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation" (Committee on National Security Systems [CNSS], 2010). Usability and security are thought to be at odds because there are few examples of the two properties being aligned. Most software, to date, has had either poor usability, poor security, or both. Both usability and security mechanisms add complexity to a system and should be designed in from the beginning, yet are often implemented as an afterthought by developers (Garfinkel, 2005). Not

surprisingly, the belief persists that if a system must be highly secured, it will not be very usable. Conversely, it is believed if a system is required to be usable, it cannot be highly secure.

From these opposing views comes one of the greatest motivators for the non-malicious insider: the need to circumvent security measures that are too difficult to use. To address this motivator, recent IA research has begun to focus more directly on making security mechanisms of information systems more usable. From this research the concept of HCI-SEC (Human Computer Interface and Security), a field of study dedicated to addressing the need for both usability and security in the development of end user applications, has emerged.

This thesis follows HCI-SEC beliefs and argues that one cannot achieve truly secure systems when the usability and/or security of a system is lacking. True security can only be realized through improving both the usability and the security of the information system (Cranor & Garfinkel, 2005). Systems that are highly secure but not very usable result in users bypassing the prescribed security features. Alternatively, highly usable systems that are not very secure are invariably compromised. Unless principles of usability and security are aligned, true cyber security cannot be achieved.

E. THE FILE-SHARING THREAT

One common IT task for which usability and security remain at odds within computer enterprises is file sharing. Employees have a personal and professional need to share information with one other, and to move information between multiple systems. Teams must collaborate on documents, subordinates must provide reports to superiors, and employees want or need to transfer files between home and office so they can work from multiple locations. These files must be shared and transferred in a secure manner. Here, our two requirements are apparent: Employees want to easily share files (usability) while the organization needs to protect these files (security). An employee's need for the most usable solution will often drive him to share files over unsecured means. For this reason, file sharing remains one of the greatest contributors to non-malicious insider threats. According to the Privacy Rights Clearinghouse, data breaches resulting from file

sharing through portable devices and unintended disclosure (e.g., sent to the wrong person via e-mail, fax, mail, etc.) led to approximately 34% of all reported data loss. In the government sector alone, these factors add up to an overwhelming 96% of reported data loss (Privacy Rights Clearinghouse, 2011). These results would seem to indicate that the inability to share files securely results in a significant risk for information systems, particularly in the federal government.

F. THESIS OUTLINE

The organization of this thesis is as follows:

- Chapter II presents a background on the research area showing how the DoD's current IA policies address insider threats. Additionally, the chapter provides a literature review focusing on major research conducted that contributes to a better understanding of the motivation behind non-malicious insider threats and the usability and security of file sharing. Finally, research supporting the evaluation methodologies developed in this thesis will be introduced.
- Chapter III provides important background information specifically addressing file sharing practices. Three basic functional requirements of a unified file sharing system are described. The historical evolution of popular file sharing technologies is presented, with an evaluation of the limitations of these legacy systems. Cloud-based file sharing is introduced along with a description of how the DoD is moving towards managing its IT infrastructure in the cloud.
- Chapter IV presents an evaluation methodology for assessing the usability and security of cloud-based file sharing technologies. This methodology involves a combination of heuristics evaluation and cognitive walkthrough. Ten heuristics are presented that are tailored to specifically address the usability and security of cloud-based file sharing systems. Three personas and ten tasks are developed as inputs to conduct a cognitive walkthrough tailored to further evaluate the usability and security of cloud-based file sharing technologies.
- Chapter V employs the usability and security evaluation methodology developed in Chapter IV to demonstrate how an evaluation should be conducted. Three popular cloud-based file sharing technologies are evaluated in an example heuristics evaluation. A cognitive walkthrough further demonstrates, using the personas and tasks developed in Chapter IV, the learnability and usability of the security features of an example technology. Finally, this chapter concludes with the results of the demonstrated evaluation showing how the three example technologies

implement the principles of usability and security required for truly secure file storage and sharing solutions.

- Chapter VI concludes with a summary of the thesis by reiterating the impact that un-usable file sharing systems can have on motivating the non-malicious insider to degrade an organization's security posture, and how the evaluation methodology developed in this thesis can be used to assess whether a solution properly aligns the principles of usability and security in its user interface. Additionally, recommendations for future research are presented.

THIS PAGE INTENTIONALLY LEFT BLANK

II. BACKGROUND RESEARCH AND LITERATURE REVIEW

A. THE NEED FOR USABLE AND SECURE FILE SHARING

Stewart (1997) stated that "knowledge has become the preeminent economic resource—more important than raw material; more important, often, than money." Information has become a primary contributor of business success in the digital age through advances in knowledge flow over internal networks, and across the Internet.

The importance of information is particularly true within the DoD, whose "business" is to ensure the national security of the United States by providing "military forces needed to deter war and to protect the security of our country" (Department of Defense [DoD], 2012a). To accomplish this mission, the DoD employs the largest workforce of any single organization in the country: 2.5 million active service members at 5,000 sites around the globe (DoD, 2012a). The IT infrastructure to support such a large organization includes over 15,000 networks and seven million computing devices (DoD, 2011). Proper command and control of such a vast IT enterprise requires the ability to collaborate on information across a multitude of networks and devices. But unlike most private organizations, the DoD's ability to make timely decisions on sharing information can mean the difference between life or death. To accentuate its need for information flow, the 2010 Quadrennial Defense Review acknowledged that "there is no exaggerating our dependence on DoD's information networks for command and control of our forces, the intelligence and logistics on which they depend, and the weapons technologies we develop and field" (DoD, 2010).

To ensure superiority over its enemies, the DoD must maintain the ability to make command and control decisions faster than its adversaries (DoD, 2007a). The acts of gathering, storing, sharing, and collaborating on information play a critical role in the decision-making process. Consequently, information sharing and processing are vital to the DoD's successfully accomplishing its "business" of maintaining national security.

B. INFORMATION ASSURANCE IN THE DOD

The ability to easily share information helps a business thrive, but information leaks to unauthorized personnel can cause a business to collapse. Within the DoD, efforts to secure information and ensure its integrity and availability comprise the DoD IA program.

1. DoD Policy Defining Information Assurance

The DoD has published policies and instructions to ensure that IA is maintained across its networks. DoD Directive (DoDD) 8500.01E, Information Assurance (IA), is the parent document to numerous service-level policies, standards, and guidelines regarding the establishment of IA (DoD, 2007b). This directive defines top-level policies governing IA across all military services and DoD agencies, as well as assigning responsibilities to individuals across DoD departments in order to ensure that these policies are followed (DoD, 2007b). Concomitantly, DoD Instruction (DoDI) 8500.2, Information Assurance (IA) Implementation, takes the policies and responsibilities prescribes by DoDD 8500.01E, and directs the implementation of security controls for information systems operating on any DoD attached network or service (DoD, 2003). Together, these documents form the IA foundation for DoD information systems. These documents are important considerations to this thesis' efforts to understand the security implications behind file sharing within the DoD.

When considering security of DoD systems, it is important to understand that some IT risk is unavoidable. It is simply not possible to implement and enforce IA measures that completely mitigate all IT risk. The goal of DoD policy is therefore to balance risk against cost, staffing levels, training requirements, and impact on mission.

Taking into account these limitations, DoDD 8500.01E requires "an appropriate level" of IA that balances the security of sensitivity information against cost effectiveness. Instead of risk elimination, enforcing IA across the DoD is a matter of risk management, i.e., a process of "identifying risk, assessing risk, and taking the steps to reduce risk to an acceptable level" (Stoneburner, Goguen, & Feringa, 2002, p. 1).

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30 enacts guidelines for managing IT-related risk and is applicable to all federal organizations that process sensitive information (Stoneburner et al., 2002). It defines threats, vulnerabilities, and impacts as key elements that must be understood to properly manage risk. In particular, "risk is a function of the likelihood of a given threat-source's exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization" (Stoneburner et al., 2002, p. 8).

Security controls are measures "that have been implemented, or are planned for implementation, by the organization to minimize or eliminate the likelihood (or probability) of a threat's exercising a system vulnerability" (Stoneburner et al., 2002, p. 19). As it is unreasonable to eliminate all risk, residual risk describes the risk remaining after new or enhanced security controls are implemented (Stoneburner et al., 2002). In summary, Figure 1 illustrates the balance of elements affecting risk within IT systems.

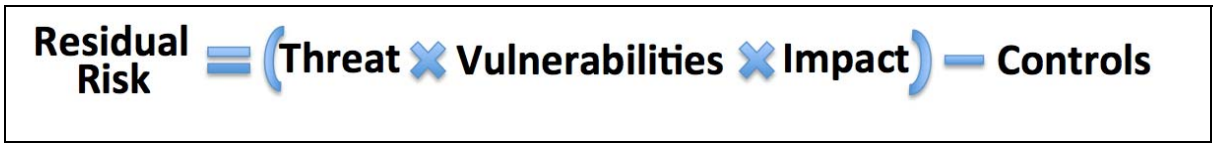

Figure 1. Summary of the elements of risk

Figure 1 depicts how security controls can be implemented by the organization to mitigate the overall risk to information. Applying security controls specifically to known threats, vulnerabilities, or their impacts will ultimately reduce the system's residual risk.

The ability to store and share files introduces vulnerabilities that must be understood in order to apply the appropriate controls that mitigate their associated risk. This thesis adheres to NIST SP 800-30 guidance to properly evaluate the severity of vulnerabilities present in current file sharing and collaboration solutions, and ultimately recommends solutions that most effectively minimize IT risks to DoD networks.

In recent years, the DoD has seen an overwhelming need to strengthen its defenses in cyberspace, in order to protect the information it shares across this realm.

The 2010 United States (U.S.) National Security Strategy stated, "cybersecurity threats represent one of the most serious national security, public safety, and economic challenges we face as a nation" (White House, 2010, p. 27). In response, the DoD has increased its focus on the war within cyberspace by establishing "Cyber" as a stand-alone warfighting domain, on par with naturally occurring domains of land, sea, air and space (DoD, 2010). United States Cyber Command was established in 2009 with a mission "to defend the information security environment" (United States Strategic Command, 2011, Focus, para. 1). Subsequently, the DoD Strategy for Operating in Cyberspace (DoD, 2011) was released, and establishes a greater emphasis on IA policy and implementation in the DoD. The strategy declared that threats to information "may be the most pervasive cyber threat today" (DoD, 2011, p. 4).

2. DoD Policy and the Non-malicious Insider Threat

Threats are any "circumstance or event with the potential to adversely impact organizational operations, organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service" (CNSS, 2010, p.75). Human threats may exist both on the outside and inside of the DoD defensive perimeter. In this context, an *outsider threat* is some "entity outside the security domain," (CNSS, 2010, p. 52) while an *insider threat* is one "with authorized access, i.e., within the security domain" (p. 38).

Insider threats, the focus of this thesis, can be further divided into those with malicious or those with non-malicious intentions. Malicious insiders often exploit their access at the "behest of foreign governments, terrorist groups, criminal elements, unscrupulous associates, or on their own initiative" (DoD, 2011, p. 3). Conversely, non-malicious insiders may threaten information systems without malicious intent toward the organization. Non-malicious insiders are typically well-intentioned employees trying to help achieve the goals of the organization, yet who may circumvent IT security controls, inadvertently causing harm to the organization. Non-malicious insiders make up the

majority of insider threats within most organizations, including the federal government (Privacy Rights Clearinghouse, 2011; Open Security Foundation, 2011).

Current DoD policies do little to address non-malicious insider threats. DoD 8500.01E declares "internal misuse" as an element that can threaten the IA of DoD operations, and indicates that system transactions shall be monitored "to detect, isolate, and react to" such threats (DoD, 2007b, p. 7). DoDI 8500.2 addresses insiders only to the extent that insider threats can be an avenue from which an adversary can attack a target. Consequently, it states that controls should be established on information systems to ensure insiders have the appropriate clearance level and need-to-know for the information being accessed (DoD, 2003). This is the extent to which these top-level policy documents address insider threats in the DoD, and no explicit discussion is provided on non-malicious insider action, nor are any security controls suggested to address the threat. NIST SP 800-30 identifies insiders as a credible threat source that should be accounted for in proper risk management, yet it fails to acknowledge these threats could have unintentional, or non-malicious motivations (Stoneburner et al., 2002).

The 2011 DoD cyber strategy improves on these earlier IA policies and instructions by placing a greater emphasis on the growing threat of insiders to IA. It states that malicious insider actions could have devastating consequences for the DoD and national security, and outlines several mitigation strategies to combat insider threats including better communication, personnel training, and new technologies and processes (DoD, 2011). Yet also absent from its pages is any acknowledgement of non-malicious insiders and the consequences their actions (DoD, 2011).

Federally sanctioned studies have been performed to better understand the insider threats within organizations. The U.S. Secret Service and Carnegie Mellon University's Computer Emergency Response Team (CERT) collaborated on the Insider Threat Study (ITS), a multiyear investigation to "identify, assess, and manage potential threats to, and vulnerabilities of, data and critical systems" (Computer Emergency Response Team [CERT], 2008, para. 1). ITS detailed extensive findings into the nature of insider threats, yet it failed to address the non-malicious aspect of the threat; instead it focused only on malicious insiders who "use or exceed their authorized access to information systems to

perpetrate harm to organizations" (CERT, 2008, para. 2). Subsequently, the findings of the ITS do little to further the understanding of non-malicious insider actions, or of ways to mitigate them.

Lynch (2006) explains an organizational instinct to under-emphasize harmful insider actions as an age-old "trusted tribe" (p. 11) mentality, where members of a tribe are expected to be trusted and only non-members of the tribe "should be viewed with suspicion" (p. 11). Organizations want to believe that members of their tribe (insiders) can always be trusted (Lynch, 2006). Perhaps, the DoD downplays non-malicious insider activity in an effort to deal publicly with outsider enemies (external hackers and malicious insiders) but privately with non-malicious insiders. The ITS seems to support this, when it found that "organizations may be reluctant to report on insider activity" (U.S. Secret Service & Computer Emergency Response Team/Software Engineering Institute [CERT/SEI], 2008, p. 12). In the absence of top-level DoD policy to address insider threats, each organization is left to deal with (or ignore) the threat in a decentralized manner.

3. Threats Posed by the Non-malicious Insider

The DoD may also intentionally downplay insider involvement in information breaches, since it perceives the occurrence of such events, or their resulting impact, as too minor to worry about. However, records show that they pose a real risk. The Privacy Rights Clearinghouse details that insider actions are the cause of a substantial amount of data loss, and non-malicious insiders are the primary cause of such loss (Privacy Rights Clearinghouse, 2011).

The Privacy Rights Clearinghouse maintains a database of reported data loss since 2005, currently indexing over 3000 incidences, and more than 500 million records breached (Privacy Rights Clearinghouse, 2011). The database categorizes reported incidents by organizational sectors, such as business, government, and nonprofit as well as by the source of the breach such as external hacking, malicious insiders, unintended

disclosure, and file transportation and sharing over portable devices (Privacy Rights Clearinghouse, 2011). Figure 2 summarizes the findings of all reported incidences within the database.

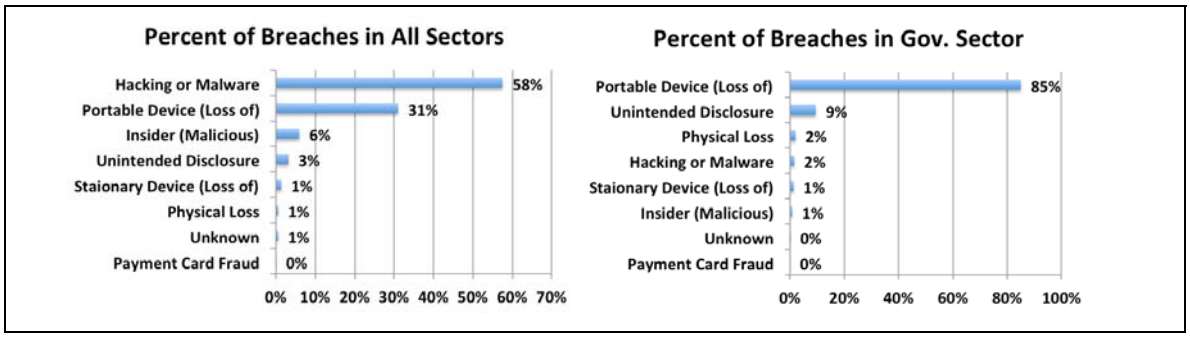

Figure 2. Reported data breaches since 2005
(From Privacy Rights Clearinghouse, 2011)

In stark contrast to the findings across all sectors, nearly all breaches within the government and military resulted from the misuse of portable devices (85%) and unintended disclosure (9%) (Privacy Rights Clearinghouse, 2011). Non-malicious insiders sharing or transporting files of information is a predominant source for both of these categories. Data breaches due to external hackers (2%) and malicious insiders (1%) were negligible (Privacy Rights Clearinghouse, 2011).

The Open Security Foundation's database of reported data loss since 2003 describes similar findings, though they do not narrow the results by business sector (Open Security Foundation, 2011). Across all sectors, data loss from external sources was still the majority at 55%, but the inside-accidental (non-malicious insider) causes accounted for 22%. Malicious insiders were only half as significant at 10% (Open Security Foundation, 2011). These findings give credence to a statement made by Morris and Thompson (1979) that, "good system security involves realistic evaluation of the risks not only of deliberate attacks but also of casual authorized access and accidental disclosure" (p. 594).

These findings show data loss with regard to personally identifiable information (PII) and do not reflect loss of operational information, such as trade secrets or classified

military information. Leaks of operational information are rarely publicized due to risks associated with professional embarrassment, loss of competitive advantage, and in the case of the DoD, threats to national security.

C. HCI-SEC (HUMAN-COMPUTER INTERACTION AND SECURITY)

Introducing data loss into a system by circumventing security measures leads to numerous consequences for non-malicious insiders, including reduced productivity, need for personnel retraining, job loss, and mission compromise. Consequently, there are few incentives for non-malicious insiders to willingly risk the consequences of not adhering to security policies and procedures. Two reasons that non-malicious insiders might circumvent security measures are:

- Lack of knowledge of a specific security measure;
- Difficulty in abiding by a specific security measure.

This thesis addresses the second reason, i.e., that insiders may threaten IA because security measures or mechanisms are too difficult to abide by or use. The idea that usability and security have been treated as opposing goals in software development is well established (Balfanz, Durfee, Grinter, & Smetters, 2004; DeWitt & Kuljis, 2006; Dourish & Redmiles, 2002; Garfinkel, 2005; Whitten, 2004; Yee, 2002; Zurko & Simon, 1996). Systems that focus on being either highly secure, or highly usable, will end up becoming neither for their users (Cranor & Garfinkel, 2005). The term HCI-SEC has emerged to define the area of research specifically seeking to align the dual goals of security and usability within modern IT systems.

1. The Problem of Cognitive Friction

The difficulty of aligning usability and security within IT systems is not surprising. Usability of IT systems in general has been difficult for humans. Human-Computer Interaction (HCI) refers to the dialog between a user and a computer needed to accomplish a task (Card, Moran, & Newell, 1983), and the field of study seeking to improve that dialog. For more than 30 years, HCI research and development has focused on designing better User Interfaces (UI) to translate user intentions into computer actions.

Many HCI researchers blame faulty interface designs for the majority of human error (Adams & Sasse, 1999; Cooper, 2004; Norman, 2002).

Cognitive friction is the resistance that the human intellect encounters "when it engages with a complex system of rules that change as the problem changes" (Cooper, 2004, p. 19). Cooper (2004) states that a major reason computer interfaces remain so difficult and error-prone is because human-software interaction is very high in cognitive friction. Norman (1983, 2002) refers to *mode error* as the difficulty humans encounter when complex devices perform different functions based on the *mode* they are in. Human error is induced if a user "believes the system is in one state (mode), when it is actually in another" (Norman, 1983, p. 255).

Cooper (2004) explains that the high cognitive friction found in IT systems is a new byproduct of the information age, where computing devices no longer provide one-to-one mapping of input to output. Cognitive friction is evident in "all software-based products, "regardless of their simplicity" (Cooper, 2004, p. 24). The complexity of computer interfaces, with the resulting cognitive friction, leads to a few principles of human behavior that are important to consider in understanding why humans may circumvent security controls (knowingly or unknowingly) in the course of interacting with a computer UI:

Users follow a path of least resistance. Zipf first articulated the principle of least effort where humans, in their quest to achieve a goal, will naturally choose the path that requires the least amount of effort (Zipf, 1949). This tendency is documented in a number of HCI studies (Cooper, 2004, Krug, 2006: Whitten, 2004; Yee, 2002). Krug (2006) described that it is more efficient to choose "the first reasonable option" (p. 24) rather than taking the time and brainpower to find the best one.

Users are goal-oriented above all. Human action is goal-oriented, and usability problems occur when human goals and the physical devices used to meet those goals do not relate well (Norman, 2002; Saltzer & Schroeder, 1975). Krug (2006) found that every interaction with the physical device "adds to our cognitive workload, distracting

our attention from the task at hand" (p. 15). Whitten (2004) observed that security is typically a secondary goal for IT users and "if security is too difficult or annoying, users may give up on it altogether" (p. 7).

Users choose trial-and-error rather than reading instructions. Krug (2006) found that most IT users are not particularly interested in "how things work, as long as we can use them" (p. 28). Additionally, when users find one method that works reasonably well they "tend not to look for a better way" (Krug, p. 28), which can lead to inefficiencies and errors that detract from security.

2. The Unusability of Security

Whereas HCI promotes better UIs to help users achieve their goals, HCI-SEC seeks to ensure that achieving user's goals is done in a secure manner. HCI-SEC argues that security is just as important to the aspects of usability as usability is important to the aspects of security (Garfinkel, 2005).

Though highly usable UI designs take great difficulty to achieve, the field of HCI has benefitted from a wealth of research. Unfortunately, this success has not translated to the field of HCI-SEC. "Usability remains one of the most pressing and challenging problems for computer security" (p. iii), observed Whitten in 2004, but the claim is still true today. Little progress has been made towards "verifiably usable security" (p. iii) despite the widespread understanding of the damaging effects of "configuration errors and other user misunderstandings" (Whitten, 2004, p. iii). Garfinkel (2005) agreed, "the topic has only rarely received significant attention as a subject of primary study" (p. 38).

Saltzer and Schroeder (1975) established some of the earliest foundational work for usable security in describing the principle of psychological acceptability. This principle promotes that:

> the human interface be designed for ease of use, so that users routinely and automatically apply the protection mechanisms correctly. Also, to the extent that the user's mental image of his protection goals matches the mechanisms he must use, mistakes will be minimized. If he must translate his image of his protection needs into a radically different specification language, he will make errors. (Saltzer & Schroeder, 1975, p.1283)

Sadly, though identified in 1975, the usability of security was neglected for many years (Whitten, 2004; Yee, 2002) despite the fact that "many security researchers have long considered usability issues, and usability researchers have long considered security issues" (Garfinkel, 2005, p. 38). Few documented works of research in HCI-SEC can be found leading into to the 21st Century (Garfinkel, 2005). This lack of research is particularly critical since many existing HCI design principles cannot be applied directly to security design elements. Whitten (2004) emphasized, "many crucial usability problems in computer security are fundamentally different from those in most other consumer software, and usability design techniques need to be carefully adapted and prioritized in order to solve them successfully" (p. 2). The need for more security specific HCI research was necessary.

Norman (1983) defined classes of human error (slip errors in particular describe non-malicious insider behavior) and established design principles to counter them. Adams and Sasse (1999) identified the lack of user-center security design as the culprit behind why users compromise security mechanisms. Whitten and Tygar (1999) emphasized this point in their study of Pretty Good Privacy (PGP) 5.0, highlighting how the software's security features remained unusable after years of UI improvements and how these unusable security features led to user error.

The new decade brought greater security threats as well as more research in HCI-SEC. In 2002, Yee's work advocated for security design from a "user-centered point of view" (p. 1) wherein actors (users) and actions (tasks) are the primary focus. His work provided ten ad-hoc principles necessary for secure interaction design (Yee, 2002). Whitten (2004) argued that verifiable usable security fails to become a reality because security design is "qualitatively different" (p. iii) than that of other types of software, and he proposed new UI design methods that specifically address such challenges. Cranor and Garfinkel (2004) edited an Institute of Electrical and Electronics Engineers (IEEE) Security and Privacy issue dedicated to security and usability with contributions from 13 prominent HCI-SEC researchers. In 2005, Garfinkel argued that usability and security can be "synergistically improved" (p. 3) to coexist and presented numerous design principles and patterns to better align them. Later, in 2005, Cranor and Garfinkel edited

and published the works of over 50 HCI-SEC researchers under the premise that "today's security problems can be solved only by addressing issues of usability and human factors" (Abstract). This collection of research in the field marked a turning point in the limited amount of research for the developing and vital field of HCI-SEC (Cranor & Garfinkel, 2005).

Further evidence of a turning point in research interest in HCI-SEC, the first annual Symposium on Usable Privacy and Security (SOUPS) was held in 2005 (http://cups.cs.cmu.edu/soups). It has since become a leading research conference exclusively promoting scholarly work to improve the usability of privacy and security. SOUPS annually presents over a dozen peer-reviewed works of research to further the body of knowledge surrounding HCI-SEC.

D. FILE SHARING RESEARCH

Tools that enable users to easily and securely share files vary greatly in their levels of usability and security. E-mail is the file sharing tool of choice for most IT users, because it is readily available and simple to use (Dalal, Nelson, Smetters, Good, & Elliot, 2008; Johnson, Bellovin, Reeder, & Schechter, 2009; Voida, Edwards, Newman, Grinter, & Ducheneaut, 2006; Whalen, Smetters, & Churchill, 2006); yet e-mail has inherent security vulnerabilities that make it a poor choice for sharing sensitive data (Johnson et al., 2009; Smetters & Good, 2009). Other options for sharing files authorized within the DoD include use of shared folders, Microsoft SharePoint, and recordable CDs. Additionally, Universal Serial Bus (USB) drives, banned within DoD in 2008, were re-authorized for restricted uses in 2010 (U.S. Strategic Command Public Affairs, 2010).

Current file sharing solutions do not always address the sharing needs of typical users (Dalal et al., 2008; Voida et al., 2006; Whalen et al., 2006). Whalen et al. (2006) observed, "even in a highly technically competent group, with good technical support, problems arise regularly, leading to frustration and difficulty" (p. 1520). As a result, users who find it difficult to achieve their work tasks may decide to circumvent prescribed sharing systems (Johnson et al., 2009), or the security measures present in the prescribed sharing system.

Exacerbating this problem is the fact that sharing files requires a user to make several critical decisions, each of which can introduce vulnerabilities in the protection system.

1. What Must be Shared?

The decision of what file to share seems straightforward; however, if done incautiously, it can present new security risks. Users often over-share files, or do not delete files that no longer need to be shared (Dalal et al., 2008; Smetters & Good, 2009). Good and Krekelberg (2003) found fewer than 10% of participants in their study were able to correctly determine which of their files and folders were being shared. If the sharing mechanism does not make users "clearly aware of what files are being offered," (Good & Krekelberg, 2003, p. 139) unauthorized disclosure of personal or professional information could result.

2. With Whom Must a File be Shared?

Access controls defines whom a file can be shared with, and what permissions the recipient has over the file being shared. Access controls are perhaps the most complex aspect of file sharing, thus it receives the majority of research emphasis. Complex access controls, while offering a great deal of restrictive control, come "at the cost of potentially high user effort and tendency for error" (Smetters & Good, 2009, p. 1). Studies of audited access control practices found that users set permissions explicitly on only a small minority of documents and folder, and instead prefer to rely on the default permissions of the system (Smetters & Good, 2009; Whalen et al., 2006). They also found that access permissions were not set once and left alone, but "changes in the work environment, as well as the need for short-term sharing, will require people to repeatedly interact with access control settings over time" (Whalen et al., 2006, p. 1519). Good and Krekelberg (2003) pointed out that the ability to stop sharing files was equally as important as the ability to share files, yet the process of revoking access control is difficult in many file sharing solutions.

3. What Mechanisms should be Used for Sharing?

An important decision that a user must make is which mechanism to use for sharing files. Voida et al. (2006), in a study of the affordances presented by a number of sharing solutions, found that "selecting a sharing mechanism with the desired features that was also available to all sharing recipients" (p. 224) led to a notable breakdown in the sharing process. Though numerous methods are available, each affords different limitations in their scope and capabilities. They found the affordance of scope, i.e., the ability to share with the most people, was the predominant motivator for why users chose a particular mechanism (Voida et al., 2006). Further, they found e-mail to be the default backup solution for most users as it was the most universally available (Voida et al. 2006).

4. The Need for Functionality to Match User Needs

Beyond the what, whom, and how of file sharing, functional flexibility is an equally important element. Whalen et al. (2006) found that end users have complex policy needs that change over time, and were inadequately addressed by current file sharing and access control mechanisms. Current solutions such as e-mail and shared folders have been used for years within organizations, yet these have been unable to adapt to users changing file sharing needs in the information age. Human research studies indicate that users require a much more flexible solution than current systems provide (Dalal et al., 2008; Johnson et al., 2009; Voida et al., 2006).

Voida et al. (2006) found that users varied substantially in their individual affordance needs for file sharing tools, as well as their willingness to share files. They detail several affordance which users require the most and compared various sharing mechanisms to determine the extent to which each met users' needs (Voida et al., 2006).

Johnson et al. (2009) also understood that current solutions did not meet users flexible affordance needs. Realizing e-mail's ease-of-use, they sought to better understand users sharing needs in an effort to "make Windows shared folders as easy to use as it is to attach files to email" (Johnson et al., 2009, p. 1). They found that systems

with restrictive centralized access control hinder "productivity and give individuals less incentive to participate in the system," (p. 1) essentially forcing them to opt for less secure alternatives (Johnson et al., 2009). To better meet the file sharing needs of users, they formalized a set of requirements called Laissez-faire sharing, defined by the properties of ownership, freedom of delegation, transparency, dependability, and minimal friction (Johnson et al., 2009).

Dalal et al. (2008) similarly found that current file sharing solutions did not provide for the complex and transient sharing needs of corporate employees, who "regularly bypass secure access procedures by using public web repositories, personal e-mails, and USB drives to transfer information" (p. 5) all in an insecure manner. They describe a more flexibile form of ad-hoc guesting that limits impedance matching when file sharing, supports ad-hoc sharing, eliminates over-sharing, and ensures user interaction with the system is simple and self-contained (Dalal et al., 2008).

E. PERSONAS AND COGNITIVE WALKTHROUGHS

Based on available solutions for storing, sharing and collaborating on files, this thesis shows that popular cloud-based solutions provide more usable security than currently approved solutions within the DoD. It does this by evaluating and comparing the usability and security of current solutions, using a method of persona development as well as task-based cognitive walkthroughs. The evaluation criteria used for the walkthroughs are based on usability and security principles established in HCI and HCI-SEC research.

1. Personas

Cooper (2004) described a user-centered design method to replace the inadequate software design methodologies prevalent in software development. His Goal-Directed design method involved the use of *Personas*, and has become extremely effective in the development of more usable computer interfaces. Personas are conceptual "people" who precisely describe a particular user of a system, and the goals the user wishes to achieve through the system (Cooper, 2004). Although personas are imaginary, they are based on

"knowledge of real users" (Calabria, 2004, What are personas?, para. 2) and should be defined "with significant rigor and precision" (Cooper, 2004, p. 124). There are practical benefits for designing with personas rather than actual users such as avoiding user's bias towards bad design and requirements creep stemming from user's wants rather than needs (Calabria, 2004; Cooper, 2004).

To ensure good persona development, personas should be as specific as possible to a given task. One should start with a name, and then build a specific history for the persona, detailing such specifics as skills, motivations, and desired goals (Calabria, 2004; Cooper, 2004). Understanding the user's goals can help in designing a system that aids the person in achieving those goals, rather than hindering them. The objective is to build systems that "bend and stretch and adapt to the user's needs," rather than the other way around (Cooper, 2004). After personas are developed and their goals are established, Cooper's (2004) method calls for the development of task scenarios, which are a "concise description of a persona using a software-based product to achieve a goal" (p. 179). Personas are run through chosen tasks to evaluate a system design. The evaluator, acting for the persona, must inhabit the character and perform the task as the persona would. The emphasis of a persona and task design on the user's goals is an important approach, since the motivation behind non-malicious insider circumvention of security controls often stems from ill-designed security measures that make it difficult for users to achieve their goals.

2. Cognitive Walkthrough

The *cognitive walkthrough* concept is a natural complement to the use of personas, goals, and task-based scenarios, and is a common evaluation approach used in HCI-SEC (Good & Krekelberg, 2003; Whitten & Tygar, 1999). Based on the early work of Wharton, Rieman, Lewis, and Polson (1994), the goal of a cognitive walkthrough is to evaluate "a design for ease of learning" (p. 1). This method of usability testing reflects the human tendency towards trial-and-error; in this context, IT users choose not to invest time for formal training or reading manuals, but opt instead to learn a system's functionality through exploring the UI (Krug, 2006). Additionally, ease of learning

addresses the goal-oriented nature of humans where users typically choose to learn about how to use new features of a system "only when their work actually requires them" (Wharton et al., 1994, p. 1). Finally, evaluating ease of learning accounts for the human need to follow a path of least resistance by allowing the costs of discovering a new feature to be balanced by the "immediate benefit to the user" (Wharton et al., 1994, p. 1).

3. Usability and Security Heuristics

Cognitive walkthroughs are limited by their narrow focus on only one aspect of usability: ease of learning. However, it is important to include other significant aspects of usability and security not inherently covered by cognitive walkthroughs. This thesis develops a framework of usability and security heuristics for file sharing, based on principles recommended by the HCI and HCI-SEC communities. This framework is introduced in Chapter IV, then used to evaluate current file sharing solutions through personas and cognitive walkthroughs in Chapter V.

THIS PAGE INTENTIONALLY LEFT BLANK

III. CURRENT FILE SHARING TECHNOLOGIES

The purpose of this thesis is to evaluate leading cloud-based file sharing technologies with respect to the usability and security features they provide to the end-user. This chapter provides a brief evolution of legacy and current file sharing technologies, and introduces emerging cloud-based solutions as having strong potential to provide a more optimal solution for the DoD and its users.

A. BASIC FUNCTIONAL REQUIREMENTS

Before we describe the evaluation criteria that will be used to determine which technology provides the appropriate balance of usability and security, we define three functional requirements of any viable file sharing solution; namely, storage, sharing, and collaboration:

- Storage provides users with a repository for files of information. Optimal storage solutions will provide user-friendly, ubiquitous access to stored files that can be synced across a wide range of devices.
- Sharing provides users the ability to extend file access to other users, and to themselves at other locations. An optimal solution affords the ability to share files with a large number of recipients, both within and beyond geographic boundaries, as well as versatile access controls that are easy to understand and implement.
- Collaboration provides users the ability to work together with others on the same document through mutual accessibility and version control. Optimal affordances for collaboration include easy-to-understand versioning, the ability to easily audit changes made to a document, as well as the ability for multiple contributors to work together on a file in near real-time (synchronously).

We are interested in recommending solutions for further evaluation that provide optimal capabilities for file storage, sharing, and collaboration. This chapter describes a number of file sharing solutions that currently are, or could be, used within the DoD. Each solution will be evaluated on its ability to provide these three basic functions. This thesis will claim that all three are necessary in an ideal solution, and will suggest a solution that optimally provides them.

B. THE EVOLUTION OF FILE SHARING TECHNOLOGIES

Before file sharing emerged within the DoD, all information that users needed was stored on local storage drives. When a user needed to access a file, the computer pulled the information from a local drive for processing. Users in disparate locations collaborated by sharing access to local files using cumbersome remote access networks. File sharing solutions were developed to enable multiple users to collaborate more easily on files of information by transporting them between each other.

1. Removable Media Solutions

Removable media describes file storage that can be easily removed from a computing device without disrupting the operations of the device. This method of file sharing is informally referred to as "sneakernet," indicating the need to physically transport the data stored on the media. Floppy disks, developed in the late 1960s, have been a dominant removable media for sharing files. Later technologies such as ZIP drives and CD-ROMs complemented the use of floppy disks for sharing files. USB flash-based storage drives, introduced in 2000, have become a popular and ubiquitous removable media file sharing method today.

USB flash-storage drives provide data storage capacities on flash memory, integrated into a USB interface. They have become popular with consumers because of their small size and relatively large data storage capacities. Modern operating systems (OS) are pre-installed with drivers that enable them to automatically mount USB drives, making them highly portable across devices.

Sharing files with USB drives is limited by time and geographic distances since they rely on sneakernet to physically transport the files. Additionally, sharing files in this manner does not scale well beyond a single recipient. Finally, collaborating via USB drives is limited by its asynchronous editing capabilities with possibly long delay times to physically transfer the files between collaborators, and the lack of automatic version tracking.

The most important limitation of USB drives in the DoD context is the additional security threats they pose to enterprise networks through their automated integration with OSs. By default, the Microsoft Windows AutoRun feature allows USB drives to automatically execute code embedded on the devices when inserted. In 2008, a virus was exposed to the DoD network that used a USB drive's portability and Windows' AutoRun automatic mounting feature to quickly spread across the enterprise, eventually crippling the DoD network (Lynn, 2010). In the wake of this incident, the DoD banned the use of USB drives for two years. In 2010, the DoD lifted the ban, but left behind strict limitations on the use of USB devices. Currently, "only government-procured and owned devices are allowed" (para.5) and are "limited to mission-essential operations, and only after strict compliance requirements are met" (U.S. Strategic Command Public Affairs, 2010, para. 6).

While USB drives provide a good means of storage, their limitations for sharing and collaborating on files, as well as their increasingly common use for spreading malware attacks (Symantec, 2009), make them a suboptimal solution for DoD users.

2. LAN-Based Solutions

In the late 1980s, advances in networking allowed organizations to connect personal computers with local area networks (LAN). These networks provided the ability to virtually share files across the LAN rather than physically. Technologies like SANs and file servers enabled the centralized storage and management of files across a networked domain. Files and folders stored on SANs can be accessed by any user logged onto the network. Access controls within the OS were used to manage the access that individuals had to the files and folders on a SAN. Windows shared drives, a dominant form of network shares on Windows-based enterprises, are a recommended and commonly used means of LAN-based file sharing within the DoD today.

Window's shared drives provide users a centralized place on the network to store a file, or folder of files, that can be accessed by all computers attached to the LAN. Any authenticated network user can have access to files stored on a shared drive. Highly configurable access controls enable both network administrators and end users to set

access restrictions on the folders and files residing on the shared drives. Johnson et al. (2009) describe several desirable attributes that Windows shared folders provide for file storage, sharing and collaboration. Shared folders relieve version tracking complications by providing collaborators access to only the most recently saved copy of a file (Johnson et al., 2009). They also provide mechanisms that prevent versioning conflicts by preventing simultaneous editing (Johnson et al., 2009). Additionally, they provide space efficiency since only a single copy of a document must be stored between all collaborators (Johnson et al., 2009). Finally, shared drives can be a highly secure place to store company files if they reside behind a corporate firewall with robust access controls.

Despite these advantages, Johnson et al. (2009) also found that the complex access control interfaces provided by Windows shared drives introduce "significant friction" (p. 4) for end users. Reeder and Maxion (2005) confirm these findings and add that Windows access controls led to a high level of user permission errors (Reeder & Maxion, 2005). The difficulty of such security measures may drive users to use less secure means of file sharing (Johnson et al., 2009; Whitten, 2004). Additionally, collaboration using Windows shared folders is limited to asynchronous editing and lack mandatory version tracking. Finally, sharing and collaboration over LAN-based Windows shared folders are typically limited by the logical boundaries of the network on which they reside. These boundaries can be extended using virtual private network technology; however, within the DoD, they typically only extend across a military installation or a small collection of installations and cannot easily serve a DoD-wide solution, let alone collaboration between DoD and non-DoD contributors.

Microsoft SharePoint is a web-based application introduced in 2001 to fill the needs of businesses for content and document management. SharePoint is most often used within the DoD as a local intranet-based portal and enterprise-wide content and document manager, but it can also be deployed to support private extranets (web-facing extensions of a corporate intranet) and Internet content management; therefore, it can be deployed as a viable cloud-based solution.

While SharePoint was developed to meet numerous enterprise level IT requirements, this thesis specifically evaluates its capabilities for file storage, sharing and collaboration. Over the past several years, SharePoint has slowly been deployed across the individual DoD enterprises and pushed as the de facto standard for file management. Therefore, it is important to fully evaluate the usability and security of SharePoint to determine if it is an appropriate solution for the DoD.

3. Internet-based Solutions

We refer to Internet-based solutions as those that provide sharing functionality over the connectivity of the Internet, where IT products and services that provide sharing are either decentralized across the Internet, or centralized within an organization's LAN. A few of the most popular Internet-based solutions include file transfer protocol (FTP), peer-to-peer networks, and e-mail. FTP provides users with simple functionality to download files from, or upload files to, a centralized location (e.g., file server), however it has not been widely used within DoD networks. Peer-to-peer networks allow the sharing of files and peripherals across the Internet via direct communication between connected computers rather than through a central server. Such networks are often maliciously abused for transferring illegal content and malicious code; therefore, they are generally not authorized on DoD networks.

E-mail is the most popular means of sharing files across the Internet (Dalal et al., 2008; Johnson et al., 2009; Voida et al., 2006; Whalen et al., 2006), and is widely used within the DoD. Since e-mail messages with attached files can be both sent and archived, e-mail is a popular means of file sharing, collaborating, and long-term storage. Not limited by the logical or geographical boundaries of a LAN, e-mail provides a highly reliable and distributed platform, and it removes the cognitive friction of complex access controls that might otherwise discourage its use.

Despite its usability, e-mail has significant drawbacks. E-mail servers and clients often limit the size of attached files, precluding sharing of large files (Dalal et al., 2008). Like USB drives and Windows shared folders, collaboration through e-mail is limited to asymmetric editing. Versioning in e-mail is possible through good management of an e-

mail chain, but the effort is not automated and can be overly cumbersome if inboxes are not properly organized. E-mail is also not an ideal solution for storage since files remain attached to disparate e-mails that may be difficult to organize and sort. Additionally, storing files in e-mail leads to file duplication since many e-mail servers store separate copies of the same file for each recipient (Dalal et al., 2008).

An important security limitation is that e-mail does not provide the ability to revoke access to a file once granted (Smetters & Good, 2009). Files attached to e-mails cannot be reliably recalled once a message is sent, and further access to the file cannot be denied without the use of a digital rights management system. Additionally, the ease of use of e-mail often leads to the inadvertent disclosure of information to unintended recipients. Such limitations in its storage and collaboration capabilities, as well as its inherent security deficiencies, preclude e-mail from being an ideal file sharing solution on DoD networks, despite its widespread use.

4. Cloud-based Solutions

Cloud computing, as defined by Mell & Grance (2011), provides "ubiquitous, convenient, on-demand network access to a shared pool of configurable computer resources" (p. 2) including networks, servers, storage, applications and services. Due to the "wide range of benefits" (p. 7) cloud technologies provide, U.S. government leadership has implemented a "Cloud First" (p. 7) policy for federal government IT management, including "using commercial cloud technologies where feasible" (Kundra, 2010, p. 7). Additionally, the National Security Telecommunications Advisory Committee (NSTAC), in its 2012 advisory report to the President of the United States, listed the capabilities found in current cloud-based file sharing technologies (e.g., *Document Collaboration*, *Project Coordination*, and *Data Archiving and Storage)* as "mission functions which appear most attractive for cloud migration" and "should be considered for earliest programmatic action" (p. 45).

Subsequently, the DoD published its own Cloud Computing Strategy indicating that it will "leverage commercially offered cloud services that offer the same or a greater level of protection necessary for DoD mission and information assets" (2012). For the

DoD, and all federal agencies, to leverage the availability of commercial Cloud Service Providers (CSP) while maintaining the strict security measures required within the federal government, the Federal Risk and Authorization Management Program (FedRAMP) was established in June of 2012 as the result of close collaboration between numerous federal agencies and private industry (http://www.fedramp.gov). FedRAMP provides a "standardized approach to security assessment, authorization, and continuous monitoring for cloud-based service" (FedRAMP, 2012, p. 2).

This move towards cloud-based technologies is due to the organizational benefits they enable, including IT systems that are efficient, agile, and innovative (DoD, 2012b). Cloud-based file sharing technologies utilize a shared pool of storage resources, remotely connected through the Internet, to provide users a highly scalable and globally accessible solution for file storage, sharing, and collaboration. These solutions combine, and improve upon, the functional benefits of legacy solutions.

Cloud-based solutions improve upon the boundary limitations of LAN-based solutions in several ways. First, the connectivity of the Internet allows users to access their files from anywhere in the world with an Internet connection. Files are no longer tied to the logical boundaries of the LAN. Further, accessibility is expanded to any device with a web browser (desktop or mobile) regardless of the OS. Finally, many cloud-based services automatically synchronize files between remote data stores and local hard drives to ensure availability during network outages.

Cloud-based solutions provide the same file sharing ease-of-use as e-mail, while improving upon its access control limitations. Cloud-based solutions typically provide access controls that allow a sender to restrict a recipient's use of stored information, as well as the ability to revoke access when needed. Additionally, because a link to the file can be shared in cloud-based solutions, rather than the file itself, server storage limitations and security concerns associated with passing files through e-mail are mitigated (Nelson, Dinolt, Michael, & Shing, 2011).

Cloud-based solutions improve upon previous collaboration methods in a number of ways. First, cloud-based solutions not only synchronize changes made to a document

by multiple users, but also provide automatic version control for these changes. This reduces human error associated with manual ad hoc versioning, and increases the likelihood that previous versions can be found. Additionally, some cloud-based services allow end users to audit the access controls in place on a file. User-accessible auditing allows users to determine what files they are sharing, and with whom, as well as who has accessed and modified their files. These capabilities are not possible with USB drives or e-mail, and only available to system administrators in Windows shared drive deployments. Services may also provide synchronous and/or asynchronous methods of collaboration, enhancing real-time productivity.

Finally, cloud-based file sharing solutions provide automatic off-site storage. For federal agencies, including the DoD, such off-site storage is a NIST standard in accordance with Federal Information Security Management Act (FISMA) requirements to ensure the availability and redundancy of information (Swanson, 2010). As an additional benefit, cloud-based technologies transport the information typically with strong encryption, making it far more secure than an employee's automobile (Kime, 2011).

C. POSSIBLE CLOUD-BASED FILE SHARING SOLUTIONS

Numerous cloud-based file sharing solutions exist that provide functional improvements over DoD's current methods for file storage, sharing, and collaboration. Table 1 enumerates multiple cloud-based file sharing technologies and show whether each service provides the three functional requirements described in this chapter for effective file storage, sharing, and collaboration. The ability to locally *synchronize* files has been added as an additional requirement, since this capability is important for DoD users to maintain access to files in the midst of limited network connectivity. Alexa, a leading provider of global web analytics, provides traffic ranks based on a combination of daily visitors to a site and page views over the last three months. Alexa traffic rankings indicate the relative global popularity of an Internet service (http://www.alexa.com), and are provided in the table for comparison purposes.

Service	Alexa Rank	Storage	Local Sync	Sharing	Collaboration	
					Asynchronous	Synchronous
Dropbox	168	X	X	X	X	
Box	730	X	X	X	X	
Zoho	1,042	X	X	X	X	
Sugarsync	6,006	X	X	X	X	
Acronis	11,456	X	X			
Carbonite	12,300	X	X			
Mozy	20,081	X	X			
Wuala	20,802	X	X	X	X	
Egnyte	24,603	X	X	X	X	
Jungle Disk	79,209	X	X	X	X	
Cubby	83,828	X	X	X	X	
SpiderOak	147,728	X	X	X	X	
ElephantDrive	289,371	X	X	X	X	
Google Drive	N/A	X	X	X	X	X
SkyDrive	N/A	X	X	X	X	X

Table 1. Basic functionality comparison of popular cloud-based technologies

THIS PAGE INTENTIONALLY LEFT BLANK

IV. EVALUATION METHODS

As stated previously, the ultimate purpose of this thesis is to develop an evaluation methodology for assessing the usability and security affordances of cloud-based file sharing technologies for the end-user. This chapter presents the methodology, which builds off the combination of a heuristics evaluation and cognitive walkthrough. Chapter V will subsequently demonstrate the methodology using a few popular technologies.

The cognitive walkthrough method is commonly used to evaluate the usability and security of computer interfaces. Because cognitive walkthroughs are focused primarily on "one attribute of usability, ease of learning" (Wharton et al., 1994, p. 3), we incorporate an additional heuristic evaluation method (Nielsen, 2005a) in our evaluation of the four cloud-based file sharing solutions chosen in Chapter IV. Whitten and Tygar (1999) used a similar approach, combining both a cognitive walkthrough and heuristic evaluation in their analysis if PGP 5.0. In this chapter, a heuristic evaluation will determine *if* each solution provides the necessary usability and security functionality, and the cognitive walkthrough will determine *how usable* that functionality is for three different user personas.

A. HEURISTIC EVALUATION

A heuristics evaluation involves assessing the user interface "against a specific list of high-priority usability principles" (Whitten & Tygar, 1999, p. 6). This section describes the high-priority principles used for this evaluation, which incorporate security as well as usability recommendations of numerous researchers from the HCI and HCI-SEC communities. These heuristics are summarized in Table 2. While not all inclusive, these principles represent the ones most germane to cloud-based file sharing. From each heuristic, questions are derived (Table 3) to evaluate whether the file sharing technology being analyzed applies the heuristic.

#	Name	Description
1	Access Control	Employ simple, seamless, mandatory access controls based on universal identifiers
2	Appearance	Present a familiar and minimal appearance that is consistent with platform conventions
3	Cognitive Friction	Reduce cognitive friction by removing sharing inhibitors and providing shortcuts and the ability to group collaborators
4	Error Reduction	Interfaces should employ the principle of least privilege, effective warning messages, and clearly marked exits to reduce human error
5	Security Feedback	Increase user awareness through security related feedback and auditing
6	Data Ownership	Provide a strong sense of ownership through delegation and revocability
7	Automatic Versioning	Provide mechanisms for automatic versioning and conflict resolution
8	Reference Links	Utilize the benefits of e-mail through reference links
9	Ubiquitous Access	Access to files should be available online, offline, and across popular operating systems and devices
10	Security Compliance	Comply with industry standards for secure storage and handling

Table 2. Cloud-based file sharing usability and security heuristics

1. Access Control: Employ Simple, Seamless, Mandatory Access Control Based on Universal Identities

Perhaps the most important security concern for storing and sharing files in the cloud is ensuring users can reliably apply access control restrictions on files. Whitten & Tygar (1999) emphasize that security software must ensure users "are reliably made aware of the security tasks they need to perform," and "are able to figure out how to successfully perform those tasks" (p. 3). Security in cloud-based file sharing systems must guide users toward successfully employing appropriate access controls on their files.

To appropriately employ access controls, user identities must be established. These identities should be derived from universal identifiers like e-mail addresses to ensure the widest scope of sharing (Dalal et al., 2008; Garfinkel, 2005) but also must be tied to a method of strong identity authentication like Public Key Infrastructure (PKI) (Nelson et al., 2011). All actions should be attributed to these identities so all actions can

be traced back to the user responsible for the action. For usability, identities should be capable of single-sign-on (SSO) with corporate authentication to reduce the need for additional password complexities.

Discretionary access controls (DAC) enable the owner, typically, of an object data file the authority to delegate or restrict access to that object (CNSS, 2010). File sharing solutions must provide mechanisms to enforce discretionary access controls (Nelson et al., 2011). Whalen et al. (2006) recommend access controls be simple: "flexible enough to accomplish common user tasks," but not so granular that they are "confusingly complex" (p. 1522). They also recommend that changes be easy to perform and not buried under too many levels of menus (Whalen et al., 2006). Smetters and Good (2009) recommended limiting the types of permissions available, indicating they found little value in permissions beyond simple "read and write and perhaps execute" (p. 11). Finally, Whalen et al. (2006) recommended these security tasks should "fit seamlessly into [the] task at hand," (p. 1522) so applying such controls should seem like a natural part of the user workflow.

2. Appearance: Present a Familiar, Consistent, Minimal Appearance

Whitten and Tygar (1999) propose that usability of security software is enhanced when users "are sufficiently comfortable with the interface to continue using it" (p. 3). Usability requires a familiar appearance that follows consistent conventions in a minimalist appearance. For familiarity, the cloud-based file storage interface should be presented to the user as a typical file system (Nelson et al., 2011), with dialog that is expressed clearly "with words, phrases, and concepts familiar to the user" (Nielsen, 2005b, para. 3) rather than system jargon. For consistency, terms and controls used across the application should conform to platform conventions and their placement should be consistent across the application (Garfinkel, 2005; Nielsen, 2005b). Such consistency helps to reduce the memory effort required of users (Norman, 1983). Effort can be further reduced "by making objects, actions, and operations visible" (Nielsen, 2005b, para. 7) to the user and ensuring helpful instructions are visible and easily

retrievable when needed. Finally, systems should have a minimal design that removes irrelevant or rarely used information (Nielsen, 2005b).

3. Cognitive Friction: Reduce Cognitive Friction by Removing Sharing Inhibitors and Providing Shortcuts and the Ability to Group Collaborators

To counter users' tendency toward the path of least resistance, Yee (2002) recommended, "the most natural way to do any task should also be the most secure way" (p. 3). File sharing systems must remain secure while reducing the barriers that "inhibit sharing" (Johnson et al., 2009, p. 2). Cognitive friction remains a barrier in any IT system, and must be reduced to a minimum in a secure file sharing system if people are to use it over unsecured means like e-mail.

In order to reduce cognitive friction in file sharing, Dalal et al. (2008) urge development of systems that support all types and sizes of files, and only require a minimal set of tools to use the system (e.g., e-mail and a web browser). Additionally, shortcuts should be provided for experienced users to use for frequent tasks so that experienced and novice users alike are productive and satisfied (Molich & Nielsen, 1990). Finally, it is important to allow users to specify logical groups of individuals "with whom files should be shared" (Voida et al., 2006, p. 226). Smetters and Good (2009) suggest tools that "maximize the use of groups" (p. 10) to handle access controls more effectively.

4. Error Reduction: Interfaces should Employ the Principle of Least Privilege, Effective Warning Messages, and Clearly Marked Exits to Reduce Human Error

Norman (1983) claims that people will make errors so systems should be designed to be insensitive to the errors. Usable security should minimize the user's ability to make dangerous errors (Whitten & Tygar, 1999), including unintentionally sharing private files with others (Good & Krekelberg, 2003), and unintentionally deleting files permanently.

To reduce unintentional sharing, Saltzer and Schroeder's (1975) *principle of least privilege* should be followed whereby "every user of a system should operate using the

least set of privileges necessary to complete the job" (p. 1282), and "the default situation is lack of access" (Saltzer & Schroeder, 1975, p. 1282). For file sharing, only explicit positive grants of access should be allowed (Smetters & Good, 2009; Yee, 2002). This principle follows the requirement of Dalal et al. for "no oversharing" (2008, p. 5).

Nielsen (2005b) recommended error-reducing systems would "either eliminate error-prone conditions or check for them and present users with a confirmation option before they commit to the action" (Nielsen, 2005b, para. 6). Effective warning messages are expressed in plain language, precisely indicate the exact cause of problem, and recommend meaningful solutions for the user (Molich & Nielsen, 1990). They should warn users of the effects of an action before it has taken place (Yee, 2002).

Additionally, to ensure systems are insensitive to errors, actions should be reversible as much as possible (Norman, 1983). As human mistakes are unavoidable, systems should provide users "clearly marked exits" (Molich & Nielsen, 1990, p. 339) to easily leave an unwanted state. *Undo* and *redo* features should be provided (Nielsen, 2005b). Unrecoverable actions should be more difficult to perform than recoverable ones, either through warning messages or delayed execution that gives users a chance "to change their minds" (Garfinkel, 2005, p. 320).

5. Security Feedback: Increase User Awareness through Security Related Feedback and Auditing

Whalen et al. (2006) found that "setting access permissions can be difficult and error-prone" (p. 1522) and users require an easy way to see "what has been done" (p. 1522). Likewise, users often forgot "what files had been shared and with whom" (Voida et al., 2006, p. 223). Therefore, providing tools that make users clearly aware of what files are being offered is in important heuristic (Good & Krekelberg, 2003). Usably secure systems "should always keep users informed about what is going on, through appropriate feedback within reasonable time" (Nielsen, 2005b, para. 2). Others describe security related feedback as visibility (Norman, 1983; Yee, 2002), transparency (Johnson et al., 2009), and explicit user auditing (Garfinkel, 2005). These terms refer to the ability of data owners to quickly and easily discover what files they have stored in the system,

who they have shared them with (Garfinkel, 2005), what access controls have been delegated on the files, and who has made changes to them (Johnson et al., 2009). Such tools decrease errors, and increase user effectiveness (Smetters & Good, 2009).

To further improve usability through feedback, Voida et al. (2006) recommended that notifications be made available and visible to avoid the usability breakdowns they found in the lack of collaborators knowing "when new content was made available (or updated)" (p. 224). Notification should also be made available to allow data owners to answer access requests for files (Bauer, Cranor, Reeder, Reiter, & Vaniea, 2008).

6. Data Ownership: Provide a Strong Sense of Ownership through Delegation and Revocability

Johnson et al. (2009) describe file *ownership* as a core principle to "better address the file sharing needs of information workers" (p. 1). Individuals who first introduce a document into a sharing system should "not have to sacrifice rights" (Johnson et al., 2009, p. 2) of ownership to use the system. Sharing systems should also promote freedom of delegation by ensuring an owner maintains the right to delegate any or all access rights to a document, "including the right for further delegation or even full ownership" to others (Johnson et al., 2009, p. 2).

An additional right of ownership is the ability to revoke access to a file from others. Good and Krekelberg (2003) defined the ability of a user to "stop sharing files successfully" (p. 139) as an important usability feature of file distribution systems. Yee (2002) also lists revocability as a requirement for usably secure systems "wherever revocation is possible" (p. 3).

7. Automatic Versioning: Provide Mechanisms for Automatic Versioning and Conflict Resolution

Nelson et al. (2011) suggested that a mechanism for referencing versions of documents should be employed in any DoD cloud-based file storage solution to ensure that an inheritable security definition is maintained. Additionally, Whalen et al. (2006) recommend versioning to "improve methods for socially appropriate content protection"

(p. 1522). Further, automatic versioning should be used to increase group productivity by reducing the complexity and time required by collaborators to develop manual ad-hoc methods of version control, as well as increasing the likelihood that a version of a file is readily available when needed.

Equally important in a system that provides automatic versioning is a robust "mechanism to merge divergent histories together" to reduce data loss and confusion when "two inconsistent copies of a file" are found (Nelson et al., 2011, p. 163).

8. Reference Links: Utilize the Benefits of E-mail through Reference Links

To supplant users' tendency to use e-mail as a sharing medium, "any cloud service for data sharing should be at least as easy as e-mailing files" (Nelson et al., 2011, p. 163). In order to combine the usability of e-mail with the security of access control restrictions, Nelson et al. (2011) propose the use of sharing files through e-mail via reference links to the file stored in the cloud instead of attaching a copy of the actual file. Such referencing ensures "email is no longer a target for intercepting sensitive files" (Nelson et al., 2011, p. 163). Referencing also eliminates the need for e-mail attachment size limits and e-mail servers being overloaded with duplicate files. E-mail then becomes a familiar tool for users to pass files, but security and usability of storing the files is still maintained by the cloud-based service. Further, referencing a file through e-mail ensures the cloud system's sharing scope is as wide as e-mail, an important affordance for users (Voida et al., 2006).

9. Ubiquitous Access: Access to Files should be Available Online, Offline, and Across Popular Operating Systems and Devices

Growing in popularity in recent years, mobile devices (e.g., tablets and smartphones) have found their way into highly collaborative organizations, and IT departments have shifted toward a "bring your own device" (BYOD) strategy. BYOD has both productivity and usability benefits, but also poses significant security concerns for an organization (Bradley, 2011). To answer such trends, the DoD has released its own mobile device strategy, citing benefits to "improve information sharing,

collaboration" and "advance the operational effectiveness of the DoD workforce" (Takai, 2012, para. 2). Including mobile devices in IT infrastructure allows information access and collaboration to extend beyond the geographical boundaries of a desktop.

Ubiquitous access includes the ability to access files on virtually any computing device regardless of the operating system. Mechanisms should be provided to automatically sync remote and local files to ensure availability when a connection to the Internet is interrupted. Files should be accessible on dominant desktop and mobile operating systems, including Windows and Macintosh on the desktop and Android and iOS on mobile devices (Net Applications, 2012a; Net Applications, 2012b). BlackBerry OS maintains a strong presence within business organizations and the federal government and should be considered for these sectors.

10. Security Compliance: Comply with Industry Standards for Secure Storage and Handling

Voida et al. (2006) listed the "location of files during [sharing]" (p. 125) as a consideration for users when choosing a file sharing solution. For the DoD, it is important to consider where files are being stored, as well as how securely the transmission and storage of the files in the cloud are managed.

Current industry standards for secure file transfer and handling call for data in transit and at rest at the data centers to be protected with strong encryption. An additional recommendation is for the ability to maintain sole ownership of the keys used to encrypt the information, coined "pre-Internet encryption" by Gibson (2011). Further, third-party certifications (e.g., SSAE 16 Type II, FISMA, ISO 27001, FIPS 140-2, and ISO 270001) indicate a cloud-based service's compliance with industry standard security controls, management and operations. As described in Chapter III, a FedRAMP security authorization indicates a CPSs compliance with federal security requirements and should be considered for any federal organization using this thesis' methods (FedRAMP, 2012).

11. Heuristic Implementation Questions

The following questions will be used to assess whether the cloud-based file sharing solutions implement the usability and security principles of each heuristic:

1. Access Control: Employ simple, seamless, mandatory access controls based on universal identifiers
• Are universal identifiers (e.g., e-mail) used for identifying individuals for access control and sharing purposes? • Can identities be incorporated with PKI authentication for single sign-on purposes? • Do the access controls provide *read-only* and *read-write* restrictions? • Are the access controls reasonable simple, not much more complex than *read-only* and *read-write*? • Is DAC enforced by requiring users to explicitly restrict access to files or folders when sharing them?
2. Appearance: Present a familiar and minimal appearance that is consistent with platform conventions
• Is the web interface presented as a file system DoD users are likely to be familiar with? • Are terms and controls presented in natural language and consistent with platform conventions? • Are frequently used controls visible to users (e.g., not hidden under other commands)? • Does the interface adequately remove information and controls that are not needed for the tasks at hand?
3. Cognitive Friction: Reduce cognitive friction by removing sharing inhibitors and providing shortcuts and the ability to group collaborators
• Can users perform the primary functionalities of file sharing with only e-mail and a web browsers? • Are the restrictions on file types and sizes unlimited, or reasonably large? • Does the system provide shortcuts for experienced users? • Does the system support logical grouping of collaborators?
4. Error Reduction: Interfaces should reduce human error through the principle of least privilege, effective warning messages, and clearly marked exits
• Is the principle of least privilege enforced by disabling access to files by default? • Are warning/help messages expressed in plain language and provide understandable guidance to the user? • Do warning messages stop users before permanently deleting files? • Do warning messages stop users before sharing private files with others? • Are undo and redo mechanisms clearly and easily available for error-prone actions?
5. Security Feedback: Increase user awareness through security related feedback and auditing
• Are auditing mechanisms available that show what files & folders have been shared, with whom, and with what restrictions?   o Is this auditing available in a single view? • Are auditing mechanisms available to see who has made changes to a file? • Are automatic feedback notifications provided to alert collaborators when files are

initially shared with them? • Are automatic feedback notifications provided to alert collaborators when shared files have been updated?
6. Data Ownership: Provide a strong sense of ownership through delegation and revocability
• Is ownership maintained and visible when a file is shared on the service? • Can ownership of files be delegated to others? • Is a mechanism provided to revoke access to updated versions of a file?
7. Automatic Versioning: Provide mechanisms for automatic versioning and conflict resolution
• Is a mechanism provided for automatic version control by default? • Is a mechanism provided to automatically manage inconsistent versions of a file without data loss?
8. Reference Links: Utilize the benefits of e-mail through reference links
• Does the system include mechanisms to send links to files via e-mail? • Does the system provide for sending e-mails from within the service
9. Ubiquitous Access: Access to files should be available online, offline, and across popular OSs and Devices
• Is access to files automatically available on Windows and Macintosh OSs when access to the Internet is interrupted? • Is access to files available through a web interface with Internet access? • Is access to files available on IOS and Android mobile OSs with an Internet connection? • Is access to files available on BlackBerry mobile OS with an Internet connection?
10. Security Compliance: Comply with industry standards for secure transfer, storage, and handling of user data
• Is data encrypted with Secure Sockets Layer (SSL) 256 during transfer? • Is data at rest encrypted with AES 256? • Can data owners maintain exclusive control of the encryption key so the service does not have access to their data? • Is the service compliant with any industry recognized standards regulations? • Is the service compliant with FedRAMP regulations?

Table 3. Questions to assess whether cloud-based file sharing technologies implement the principles of the heuristics

B. EVALUATION PERSONAS

To conduct a cognitive walkthrough, we will employ the use of personas as described by Cooper (2004) and summarized in section 2.5.1 of this thesis. As suggested by Calabria (2005) we have developed a discrete set of personas to "satisfy all users with similar goals" (p. 4). Although all DoD users cannot be represented, the three personas listed in Table 3 contrast the most common levels of technical expertise, professional experience, and duty related goals found in the DoD in an effort to appeal to the broadest

range of users. We will describe each persona in an effort to understand who they are, what level of IT skills they have, and the motivations and goals that drive their professional duties (Cooper, 2004).

#	Name	Description
1	Chris	Tech-Savvy Young Airman
2	Bob	Seasoned Non-Commissioned Officer In Charge (NCOIC)
3	Alice	Inexperienced Commander's Secretary

Table 4. Personas used to assess the usability and security of cloud-based file sharing technologies

1. Chris, the Tech-Savvy Young Airman

Figure 3. Chris, the tech-savvy young airman

Chris is a 20-year-old junior enlisted airman serving in his first duty station at an overseas air base. He joined the service almost two years ago after working part time at a big box electronics store for a year after high school. He learned about computers in middle school and built his own during a basic computer course as a sophomore in high school. He enjoys music, video games and socializing on the web with friends back home through social media sites. Technology is his hobby and he is thrilled at the chance to try out new IT products and services, especially when they are highly configurable to fit his needs.

Chris currently works as a network operations apprentice, responsible for the maintenance and uninterrupted operations of all servers providing basic communication

services (e.g., e-mail, file servers, Internet access) to over 6,000 base personnel. He received 15 weeks of technical training for this job, but many of his skills were developed outside of formal training programs.

Though excited about the prospects of this job, he is quickly disappointed to find most of his actual tasks are mundane and effortless to him. Much of his day is spent resetting BlackBerry and Active Directory accounts, finding files on the SAN that users accidentally deleted or lost, and fixing permissions for folders on the file server. He gets tired of people complaining about lost files, or the limited e-mail space they are given.

Chris is always looking for ways to make his job more interesting, which typically involves quickly solving customers' problems so he can get back to browsing the web for new and interesting technology. But he also knows that if he can impress his boss, he has a chance of getting the coveted Airman-of-the-Quarter award and impressing his friends and family. Accordingly, he is always looking for better productivity solutions to please his boss and get off the phone with customers faster.

He is excited to hear about a new file sharing system to replace shared drive for storing and sharing files across the base. The idea that users can now handle many of their problems personally may reduce many of his monotonous tasks. Though he personally does not have to share files very often with co-workers, he has not been able to use his thumb drive due to official directives and is looking for an official way of accessing his personal files from anywhere, especially via his smart phone.

2. Bob, the Seasoned Non-commissioned Officer In Charge (NCOIC)

Figure 4. Bob, the seasoned NCOIC

Bob, a 39-year-old senior enlisted airman, has been in the military for 18 years. He came into the Air Force as a mechanic, but has been a network infrastructure operator for the last 14 years. This experience has made him somewhat of a subject matter expert (SME) in his field.

Bob has served the last 3 years as the NCOIC of the network infrastructure shop, but recently stepped up to be the section superintendent. His supervisory responsibilities have expanded beyond his shop to include network operations (where Chris works) and network security. He thoroughly enjoyed his hands-on responsibilities as the lead SME of his shop, so the transition to the management work of a superintendent has been slow. Now supervising the operations of 54 airmen across the three shops, most of his daily duties include attending meetings, answering taskers from his boss, quality checking the work done by the shops, and writing appraisals and awards for his airmen. These tasks present him with over 90 e-mails each day, 70% of which require a response. His inbox remains only moderately organized with important e-mails and files spread across half-hearted attempts to get organized. He gets aggravated knowing he probably spends nearly an hour each day just looking for lost messages and files in his inbox. He misses working face-to-face with the troops and schedules opportunities to get out of the office and visit them—even if that means skipping a lunch or two or missing a couple deadlines.

With over 14 years working with network interfaces and programming Internet protocol address ranges, his computer hardware skills are excellent. However, he feels only moderately proficient with software like the Microsoft Office suite. It can take Bob

many months to become comfortable with a new software interface, and each time he does, the Air Force seems to push down a new system to replace the one he just learned. DoD budget cuts have forced personnel reductions, so new automated systems are constantly deployed to help the remaining work force *do more with less*. But each new system requires him to learn an entirely new way of doing things. He would prefer to continue using the systems he is comfortable with.

Bob wants to look professional and be in control. As an SME for the section, he is looked to as an example for knowledge, skill, and situational awareness. Such awareness of the operations of three large shops means constantly being tapped into information. He does not want to appear stressed or frantic about the numerous deadlines he has to meet, even though he is. Additionally, he is hoping that having better control of the flight affairs will impress his boss and hopefully put him in line for a quarterly award that will gain him a few more points toward a promotion next year. He is intrigued by a new system coming that aspires to facilitate more efficient file storage, sharing and collaboration. While he sees it as an opportunity to be more productive, he is mostly anxious about the learning curve it will take to master the system.

3. Alice, the Inexperienced Commander's Secretary

Figure 5. Alice, the inexperienced commander's secretary

Alice recently found a day job as the secretary for the communications squadron commanders (where Bob and Chris work). As a 45-year-old mother of three, she is in her first professional job in several years, returning to work now that her youngest is in school. Her husband serves in the military so she has a lot of experience living with, but not working for, the military. She has never been a secretary before, so she was very

surprised to be hired. She is a fast typist, but aside from casual web surfing, she has very little experience with computers. She attributes her hiring to her very friendly and enjoyable personality. Now she has become overwhelmed with the workload required by her job. She has taken a basic online course to learn Microsoft Office, but feels she is in over her head for most of the IT related secretarial skills she has been asked to perform.

Recognizing Alice's inability to keep up with her duties, the commander brought in a temporary assistant to help. Now, Alice wants nothing more than to show confidence in her duties to build her boss's trust so that he no longer feels she needs help. Alice learns quickly, but gets frustrated when what she thinks should be a simple task becomes overly complicated by computers. Ultimately, she just wants to unbury herself from the piles of work that are growing around her.

Most of Alice's day is filled with managing the commander's e-mail inboxes and schedules and answering phone calls. She is becoming more proficient at skimming e-mail and managing his calendar, but answering the phone causes here great anxiety. Most calls are questions she rarely has the answer to. They involve questions regarding base rules and regulations, upcoming events, and overall situational awareness of things at the commander's level. Answers to these questions require access to information that she knows is available on the squadron's shared drive, but she has had very little success finding the information she needs. Further, she is concerned with how to efficiently share the information with the person requesting when she does find it. Finally, she finds it very difficult to organize her files so she can find the information again when needed. As the commander's secretary, she is required to post and share numerous command level documents onto the shared drives folders for others to use. Sometimes the information she has is sensitive and she must find a secure means of sharing the information with only specific people.

C. EVALUATION TASKS

The tasks listed in Table 5 have been developed to evaluate the usability of each cloud-based technology's implementation of the usable security heuristics in section 4.1. Task-based scenarios are a "concise description of a persona using a software-based

product to achieve a goal" (Cooper, 2004, p. 179), and are used here to describe the tasks and "actions sequences for completing the tasks" (Wharton et al., 1994, p. 2) required as inputs for a cognitive walkthrough. Following recommendations from Cooper (2004) and Wharton et al. (1994), we limit the number of tasks to those most relevant to DoD users sharing files securely.

#	Task	Evaluates
1	Add a file to the service	Familiarity with the interface appearance and functionality and overall usability
2	Organize a given folder structure	Familiarity with the interface appearance and functionality and overall usability
3	Share a file with co-works with specific rights	How easily one can share files and apply appropriate access controls to access them
4	Determine which files and folders are being shared	The availability, visibility, and usability of the feedback and auditing tools provided by the service
5	Audit collaborators actions on a file	The availability, visibility, and usability of auditing tools to determine who has accessed or made changes to a file
6	Revoke a collaborators access to a file	The availability, visibility, and usability of tools that allow revoking access to a shared file
7	Determine the access controls on a shared file	The visibility and usability of the feedback and auditing tools available at the file level provided by the service
8	Revert to an earlier version of a file	The availability, visibility, and usability of automatic versioning tools provided by the service
9	Fix inconsistent versions of a file	The availability, visibility, and usability of tools to de-conflict inconsistent versions of a file
10	Find a specific file within a large hierarchy of files	The file retrieval usability and capabilities of the service

Table 5. Cognitive walkthrough tasks to assess the usability and security of cloud-based file sharing technologies

1. Add a File to the Service

This task requires the persona to take a file from the desktop and place it on the sharing service using the tools provided by the particular sharing service, and is intended to evaluate familiarity with the appearance, functionality and overall usability.

2. Organize a Given Folder Structure

This task presents the user with the web interface of each service, preloaded with five files, and requires the persona to organize the files to match a folder hierarchy presented to the persona. This also evaluates the persona's familiarity with the interface and their ability to use the tools provided.

3. Share a File with Co-workers with Specific Rights

In this task, a persona must share a given folder with two coworkers, and delegate to each coworker a different permission level. This will evaluate how easily each solution allows the persona not only to share a file with others within the organization, but also to ensure the appropriate access controls are in place on the file once shared.

4. Determine which Files and Folders are Being Shared

This task requires the persona, presented with an intricate folder hierarchy containing over 3,000 files, to use the service's feedback tools to determine which of the thousands of files are being shared with others. This evaluates the availability, visibility, and usability of the feedback and auditing tools provided by the service.

5. Audit Collaborators' Actions on a File

Here, a persona is presented with a file that several collaborators have made changes to, and must determine who made the changes. This task evaluates the availability, visibility, and usability of auditing tools to determine who has accessed or modified a file.

6. Revoke a Collaborator's Access to a File or Folder

When a collaborator is no longer part of the team working on a particular file, they no longer require access to it. This task presents the persona with a shared file and

the name of a collaborator who no longer needs access to it, and asks the persona to remove access. This task evaluates the availability, visibility, and usability of tools that allow revoking access to a shared file.

7. Determine the Access Controls on a Shared Folder

Given a particular file with numerous collaborators having access to it, this task requires the persona to determine who has access to the file and what access modes they have, using the tools provided by the service. This evaluates the availability, visibility, usability of the feedback and auditing tools provided by the service.

8. Revert to an Earlier Version of a File

This task provides the persona with a file that has gone through several revisions. Determined that the last three changes made to a file are not to be used, this task asks users to revert to the version saved before the last three revisions. This task evaluates the availability, visibility, and usability of the automatic versioning mechanisms of each service, and how easily one can access the versions as well as revert to an older file. The only help provided to the user is the file, with no indication on how to access the versions or how to revert to older ones.

9. Fix Inconsistent Versions of a File

Inconsistencies arise when two collaborators work on and save changes to a file at the same time, creating conflicts between the versions. This task requires a persona to resolve the conflicts between the two versions using the tools provided by the service. In addition to evaluating the tool's ease-of-use, an additional evaluation will be noted about whether the service allows for retaining the changes made to both files or if some data must be lost.

10. Find a Specific File within a Large Hierarchy of Files

Users often need to find files amid a large and intricate, often unorganized, folder hierarchy. This task again presents the user with a folder hierarchy containing over 3,000 files and asks them to find a specified folder and file. This task evaluates the file retrieval usability and capability of each service.

THIS PAGE INTENTIONALLY LEFT BLANK

V. EVALUATION METHODOLOGY DEMONSTRATION

Chapter IV described a methodology for evaluating the usability and security of cloud-based file sharing technologies, using a combination of heuristics evaluation and task-based cognitive walkthrough. This chapter demonstrates how to conduct an evaluation using this methodology and provides recommendations for assessing the results. For this demonstration, we have chosen to evaluate three of the more popular cloud-based technologies as possible solutions to meet the file sharing needs of DoD users.

A. TECHNOLOGIES TO BE EVALUATED

1. Dropbox

Dropbox (https://www.dropbox.com) is the most popular web-based file sharing service, according to its Alexa rank of 168 (https://www.alexa.com). Simplicity and ease of use are two of Dropbox's heavily marked benefits. There are currently over 50 million users of Dropbox (Dropbox, 2012), including employees from 87% of Fortune 100 firms (Schadler, Brown, & Martyn, 2011). In a study of the mobility affordances of several collaboration services, Forrester Research recommends Dropbox as a "Strong Performer" in the mobile collaboration space (Schadler et al., 2011).

Dropbox was chosen for its exceptional simplicity and ease-of-use in syncing, storing and sharing files. Too often, however, ease-of-use tends to limit the security or functionality of an IT solution. Including Dropbox in this evaluation will help determine if the service delivers on its promise of usability as well as providing for the basic security needs of DoD users.

2. Google Drive

Google Drive (https://drive.google.com) is a file sharing system that also provides users an entire suite of web-hosted office productive software that supports multiple collaboration models. In additional to basic file storage and sharing, this software

improves upon collaboration by adding the capability for synchronous file editing within its web-hosted applications, allowing users to work simultaneously on the same document. The service also allows inline messaging between contributors to further enhanced collaboration.

Google Drive is provided as an enterprise service as part of Google Apps for Business. Google (2012a) claims that over 5 million government and businesses currently use Google Apps for Business including U.S. General Services Administration (GSA), Genetech, and the city of Los Angeles (Schalder et al., 2011). Forrester Research recommends Google Docs as a "Strong Performer" in the mobile collaboration space (Schalder et al., 2011).

Google Drive's was chosen for comparison because of it added collaborative functionality over Dropbox, which makes it appealing for highly collaborative environments like the DoD. Including it in this evaluation will help determine if usability and security is maintained despite the added functionality.

3. Box

Box (https://www.box.com) provides enterprise-level security and administration tools in addition to file sharing. Like Dropbox, Box promises users a simple and powerful way "to access and share their content from anywhere" (Box, 2012, Reinventing how the world uses business content, para. 1). Box also promises seamless integration with a wealth of enterprise services like SharePoint, Active Directory, and Microsoft Office as well as Google Drive's office productivity software to enable synchronous file collaboration. Additionally, Box provides numerous enterprises level security and administration features, with finer granularity than Dropbox and Google Drive.

Box claims that over 10 million individuals, small businesses and Fortune 500 companies currently use their service (Box, 2012). Forrester Research recommends Box over Dropbox and Google Docs as a "Leader" in the mobile collaboration space with the highest rankings among the services it evaluated (Schadler et al., 2011). Including Box

in this evaluation will determine if its usability and security can keep up with its added functionality and enterprise-level service integration.

B. HEURISTICS EVALUATION

This section evaluates each of the cloud-based technologies using the heuristics developed in chapter IV of this thesis. This method of evaluation utilizes questions, listed first in Table 3 and reiterated in Table 6, to assess whether a particular technology implements the principles of a heuristic. Each question elicits a "yes" response when the principle is followed and a "no" response when it is not. Table 6 presents the results of our heuristics evaluation method for the chosen technologies. Each heuristic, with its applicable questions, is shown on the left-hand column. The response to each question, i.e., whether the technology implements the principle of the question, is shown by a "Y" in the appropriate right-hand column. Empty cells, indicating the technology does not implement the particular principle of the heuristic, are highlighted with a red border for visual significance.

The heuristics evaluation is a relatively efficient and effective way to determine if a specific technology adheres to usability and security principles. The resulting table for such an evaluation shows, at a glance, the compliance and non-compliance of each technology, allowing decision makers within an organization the ability to determine tradeoffs between numerous competing usability and security goals.

		Dropbox	Google Drive	Box
1. Access Control: Employ simple, seamless, mandatory access controls based on universal identifiers				
	Are universal identifiers (e.g., e-mail addresses) used for identifying individuals for access control and sharing purposes?	Y	Y	Y
	Can identities be incorporated with PKI authentication for single sign-on purposes?		Y	Y
	Do the access controls provide *read-only* and *read-write* restrictions?	Y	Y	Y
	Are the access controls reasonable simple, not much more complex than *read-only* and *read-write*?	Y	Y	Y
	Is DAC enforced by requiring users to explicitly restrict access to files or folders when sharing them?			
2. Appearance: Present a familiar and minimal appearance that is consistent with platform conventions				
	Is the web interface presented as a file system DoD users are likely to be familiar with?	Y	Y	Y
	Are terms and controls presented in natural language and consistent with platform conventions?		Y	
	Are frequently used controls visible to users (e.g., not hidden under other commands)?			Y
	Does the interface adequately remove information and controls that are not needed for the tasks at hand?	Y	Y	Y
3. Cognitive Friction: Reduce cognitive friction by removing sharing inhibitors and providing shortcuts and the ability to group collaborators				
	Can users perform the primary functionalities of file sharing with only e-mail and a web browsers?	Y	Y	Y
	Are the restrictions on file types and sizes unlimited, or reasonably large	Y		
	Does the system provide shortcuts for experienced users?	Y	Y	Y
	Does the system support logical grouping of collaborators?			
4. Error Reduction: Interfaces should reduce human error through the principle of least privilege, effective warning messages, and clearly marked exits				
	Is the principle of least privilege enforced by disabling access to files by default?	Y	Y	
	Are warning/help messages expressed in plain language and provide understandable guidance to the user?	Y	Y	Y
	Do warning messages stop users before permanently deleting files?	Y		Y
	Do warning messages stop users before sharing private files with others?			
	Are undo and redo mechanisms clearly and easily available for error-prone actions?	Y	Y	
5. Security Feedback: Increase user awareness through security related feedback and auditing				
	Are auditing mechanisms available that show what files & folders have been shared, with whom, and with what restrictions?	Y	Y	Y
	>Is this auditing available in a single view?	Y		
	Are auditing mechanisms available to see who has made changes to a file?	Y	Y	Y
	Are automatic feedback notifications provided to alert collaborators when files are initially shared with them?	Y	Y	Y
	Are automatic feedback notifications provided to alert collaborators when shared files have been updated?	Y		Y
6. Data Ownership: Provide a strong sense of ownership through delegation and revocability				
	Is ownership maintained and visible when a file is shared on the service?	Y	Y	Y
	Can ownership of files be delegated to others?			
	Is a mechanism provided to revoke access to updated versions of a file?	Y	Y	Y
7. Automatic Versioning: Provide mechanisms for automatic versioning and conflict resolution				
	Is a mechanism provided for automatic version control by default?	Y	Y	Y
	Is a mechanism provided to automatically manage inconsistent versions of a file without data loss?	Y	Y	Y
8. Reference Links: Utilize the benefits of e-mail through reference links				
	Are mechanisms in place to share files via reference links over e-mail?	Y	Y	Y
	Are tools available to e-mail links to files from within the service	Y	Y	Y
9. Ubiquitous Access: Access to files should be available online, offline, and across popular OSs and Devices				
	Is access to files automatically available on Windows and Macintosh OSs when access to the Internet is interrupted?	Y		
	Is access to files available through a web interface with Internet access?	Y	Y	Y
	Is access to files available on IOS and Android mobile Oss with an Internet connection?	Y	Y	Y
	Is access to files available on BlackBerry mobile OS with an Internet connection?	Y		Y
10. Security Compliance: Comply with industry standards for secure transfer, storage, and handling of user data				
	Is data encrypted with SSL 256 during transfer?	Y	Y	Y
	Is data at rest encrypted with AES 256?	Y		Y
	Can data owners maintain exclusive control of the encryption key so the service does not have access to their data?			
	Is the service compliant with any industry recognized standards regulations?		Y	Y
	Is the service compliant with FedRAMP regulations?			

Table 6. Heuristics evaluation results

C. COGNITIVE WALKTHROUGH

As stated earlier, a heuristics evaluation shows *if* a technology employs the principles of each heuristic, but it does not indicate *how usable* the technology is. For the latter, a cognitive walkthrough is a good complement to a heuristics evaluation.

As described in Chapter II of this thesis, the cognitive walkthrough methodology is used to evaluate the "ease-of-learning" of a system's interface. The walkthrough takes a given task, and seeks to:

> consider, in sequence, each of the user actions needed to accomplish the task. For each action, the analysts try to tell a story about a typical user's interaction with the interface. They ask what the user would be trying to do at this point and what actions the interface makes available. (Wharton et al., 1994, p. 3)

Inputs to the walkthrough will be the personas developed in Chapter IV of this thesis (see Table 4), representing the users to be evaluated, and several of the tasks defined in Chapter IV (see Table 5), as "sample tasks for evaluation" (Wharton et al., 1994, p. 2). The walkthroughs for each of these tasks are described in the following sections. Each section summarizes the task and the usability it seeks to evaluate, followed by a detailed design description of the interface elements necessary for completing the task. Following this introduction, each persona's interactions with the technology are described to "uncover design errors that would interfere" (Wharton et al., 1994, p. 4) with the respective persona's ability to learn and use the interfaces.

While performing a cognitive walkthrough can be costly both in time, money, and human resources, our methodology uses the results of the heuristics evaluation to narrow the list of alternatives that warrant further consideration for a cognitive walkthrough. Organizations should use the heuristics evaluation table to determine the appropriate tradeoffs between the usability and security required by their organization, and select from only the most promising technologies for further evaluation.

We previously determined that Dropbox provides a good balance of security and usability for our example organization, and therefore Dropbox was used to demonstrate how a cognitive walkthrough could be used to evaluate this technology. As this chapter

is intended solely as a demonstration, only tasks 3 through 5 from Table 5 will be analyzed here. These tasks were chosen because they represent the most security-focused of the ten tasks described in Chapter IV, and therefore exhibit the usability of Dropbox's primary security-relevant interface elements.

Figure 6 shows Dropbox's main interface. Boxes are drawn to highlight the key areas that will be referenced in the interface descriptions throughout the walkthroughs.

Figure 6. Dropbox's primary interface

1. Task 3: Share a File or Folder with Co-workers with Specific Rights

This task evaluates how easily a user can share a file with a collaborator and restrict access to that file, by requiring each persona to share a given file with two coworkers and delegate different permission levels to each. Like many similar services, Dropbox provides both *read-only* and *read-write* access; however, unlike most other sharing technologies, it separates these two access modes into completely different workflows, each with their own UI and terminology.

Dropbox never uses the term *read-only* access in its interface, but provides the ability to grant such rights. In place of *read-only*, the term *links* is used as a method to provide other users access to *view* files. Sharing a file or folder with *read-only* access is done using the *Get Link* button. The *Get Link* button is hidden by default, but appears in the *contextual menu bar* (Figure 7) once a file or folder is selected, represented as a chain links icon with the label *Get Link*. Clicking on this button allows the user to provide a *read-only* link to other users to view the document or folder; other users cannot make changes through this link. *Links* can be given to anyone with an e-mail address; they need not be authenticated by Dropbox to view the file. Dropbox also does not provide the ability to restrict *read-only* rights to individuals once granted, meaning anyone who has a link to the file can view it once it has been shared in this manner, even if the owner did not explicitly share the link with them.

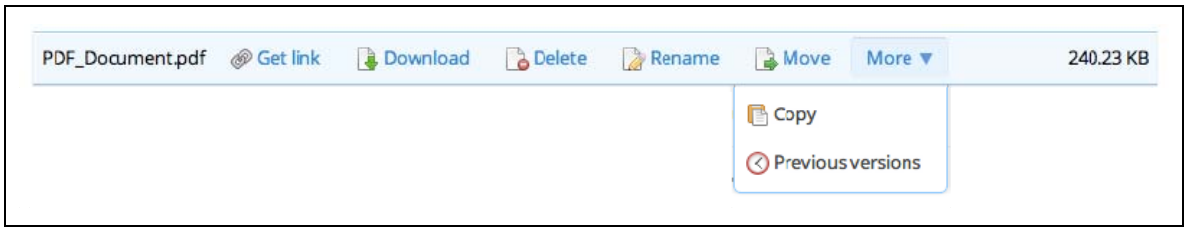

Figure 7. Contextual *menu bar* for a selected file

Dropbox also never uses the term *read-write* access in its interface, but does provide tools to grant such access. To grant *read-write* access, it uses inconsistent terms such as *inviting* others to a folder, *collaborating* on a folder, or *sharing* folders. Such *read-write* permissions are only possible at the folder level on Dropbox, and not available for individual files. Once granted *read-write* permissions, collaborators have full control of anything within that folder (including the ability to add, delete, and modify files). Dropbox does not provide more granular restrictions on individual file access or different access modes; it provides either all or nothing. Granting *read-write* permission to a folder is accomplished by clicking on the *Invite to folder* icon (a blue folder overlaid with a rainbow) that appears on the *contextual menu bar* after selecting the chosen folder (Figure 8).

Users can also share *read-write* access to a folder by clicking on the same icon in the *top menu bar*. This presents a wizard that guides the user to choose a folder to share, or create a new shared folder. Unlike the *read-only* permissions on a folder, *read-write* permissions on a folder are restricted to only those who are explicitly granted access to the folder.

Read-only and *read-write* are the only access modes available within Dropbox. More advanced modes (i.e., *execute* or *write-only)* are not available.

Figure 8. *Contextual menu bar* options for a selected folder

All methods of sharing a file or folder, regardless of *read-only* or *read-write*, utilize a wizard (Figure 9) that guides the user through providing e-mail addresses of other users with whom to share the file or folder. The wizard provides an optional message to accompany the invitation. Once sent, a feedback message, *Sent successfully*, appears at the top of the page to confirm that the file has been shared.

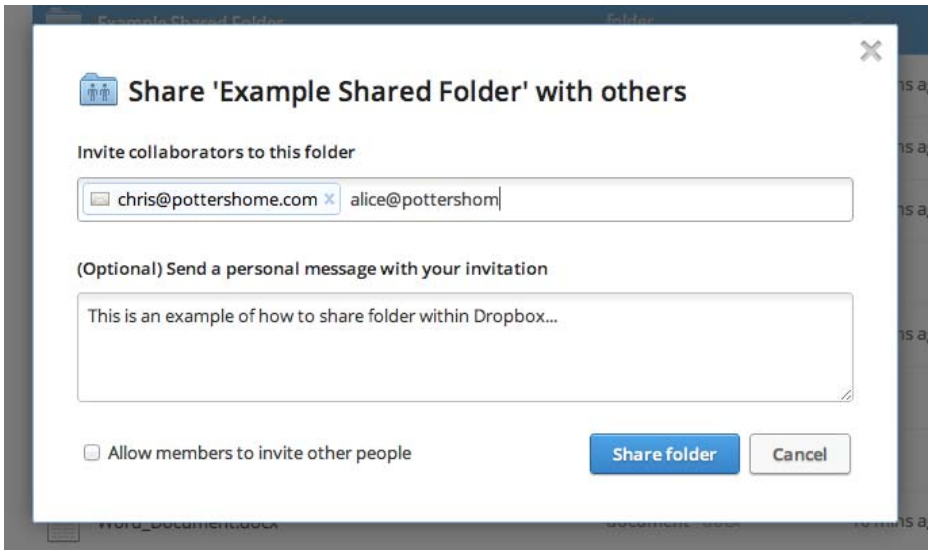

Figure 9. Share file or folder wizard

The following sections detail the interactions of each of our personas when accomplishing this task:

a. Alice, the Inexperienced Commander's Secretary

Alice is not very familiar with the traditional verbiage used for *read-only* and *read-write* permission levels, so the absence of these terms in Dropbox will not impact her. However, Dropbox does not use consistent terms to address these two capabilities and the multiple terms used (e.g., *links, view, collaborate, invite, share*) make her confused as to exactly what access she is granting to others. Only the term *share* relates directly to this task, but it is not used in Dropbox to label the tools used to accomplish this task (e.g., *Get Link* and *Invite to folder*). Having two separate workflows to accomplish the different kinds of sharing will cause a moderate amount of cognitive friction for her, since she must think about what level of permission she wants to give before she starts the sharing process. Minimal training, or significant trial-and-error, will be required for Alice to understand how Dropbox distinguishes between *read-only* and read-*write* access modes and how to apply them.

Once she finds and learns the proper tools, however, their placement is visible and consistent in the interface, and the steps required to share a file are simple and few. The pop-up window that results from both sharing methods provides dialog that is simple yet informative enough to guide Alice quickly through the process and ensure she knows which file or folder she is sharing. She only needs to know the e-mail addresses of those she wants to share the file with. The immediate feedback provided by the interface tells her that she has completed the task successfully. Learning this task initially will be highly difficult for Alice, but once learned the tools are highly useable and Alice can perform repeat the task easily.

b. Bob, the Seasoned NCOIC

Bob, like Alice, must wrestle with the distinctions Dropbox places on *read-only* and *read-write* access. Unlike Alice, he is familiar with the concepts of *read-only* and *read-write* to describe access permissions, so mapping these concepts to Dropbox's inconsistently used terms results in only moderate cognitive friction for him. He is also familiar with the convention of applying the different permission levels through a single workflow, so he must translate his conventions into two separate workflows. As with Alice, this can be learned through minimal training or trial-and-error. Bob learns the concepts with less time-consuming trial-and-error than Alice, due to his familiarity with computers, but minimal training would still help explain how to apply the different access modes appropriately as it is not apparent in the interface.

Like Alice, Bob will be able to easily use the tools once the distinctions have been learned. The dialog in the wizard is simple yet informative enough for him to feel confident in knowing which file he is sharing, and with whom. He especially appreciates the automatic look-up Dropbox performs when he shares a file with a co-worker he has previously shared, with as this feature saves him valuable time. The feedback generated once a file or folder is shared also builds his confidence that he has completed the task successfully. Bob can learn this task with moderate difficulty on the first try, but the high usability of the tool once learned enables him successfully repeat the task easily.

c. Chris, the Tech-savvy Young Airman

Though he is normally very technically savvy, the different workflows for applying different permissions will initially be difficult for Chris for the same reasons they were for Alice and Bob. Chris' background with computer jargon and his exploration of several emerging web-based system will help him to understand the distinctions quickly through minimal training or limited trial-and-error. Once learned, Chris can easily and reliably repeat the task successfully. The ease of learning this task for Chris is still a cause of friction, but the high usability makes proficiency easy for him to achieve after minor initial effort.

2. Task 4: Determine which Files and Folders are Being Shared

This task evaluates the availability, visibility, and usability of feedback tools by requiring the persona to determine which of their files and folders are being shared with others. Dropbox excels at this task by presenting everything a user has shared with anybody within a two views: the *Links* view shows all files and folders shared with *read-only* access and the *Sharing* view shows all folders shared with *read-write* access.

The *Links* button allows users to see all the files and folders they have shared with read-*only* access. The *Links* button is found in the *left menu bar* (Figure 6), and is represented by a chain links icon with the label *Links*. Once clicked, the resulting page (Figure 10) lists all the files that are being shared with *read-only* access with when they were created, and provides a *remove* button that will revoke the *read-only* access. The page does not show whom a file is being shared with, since *read-only* access is provided to anyone with a link to the file. To increase learnability, this view provides a concise description of how Dropbox manages links in a caption above the list of files.

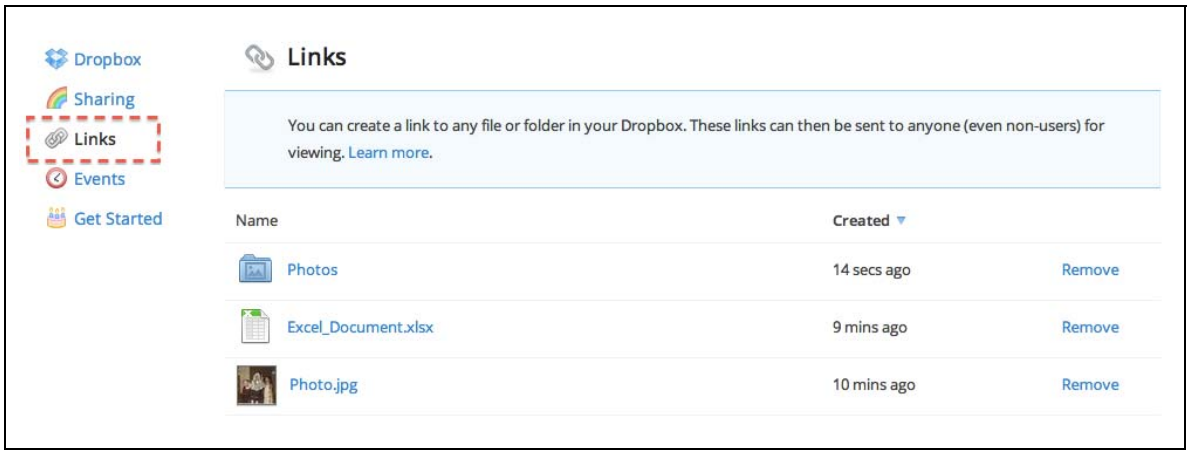

Figure 10. *Links* view shows all files and folders shared with *read-only* access

The *Sharing* view provides the user the ability to see information on folders being shared with *read-write* access, and is accessible by clicking on the *Sharing* button (with rainbow icon) in the *left menu bar* (Figure 6). The resulting page (Figure 11) lists all the folders being shared with *read-write* access, and the users each folder is being shared with. This view also displays when the last file within the folder was modified, and provides an *options* button to see additional details on who has access to the folder, or to grant or revoke access to the folder. To aid learnability, this view provides a concise statement in a caption at the top describing how the sharing of folders is accomplished in Dropbox.

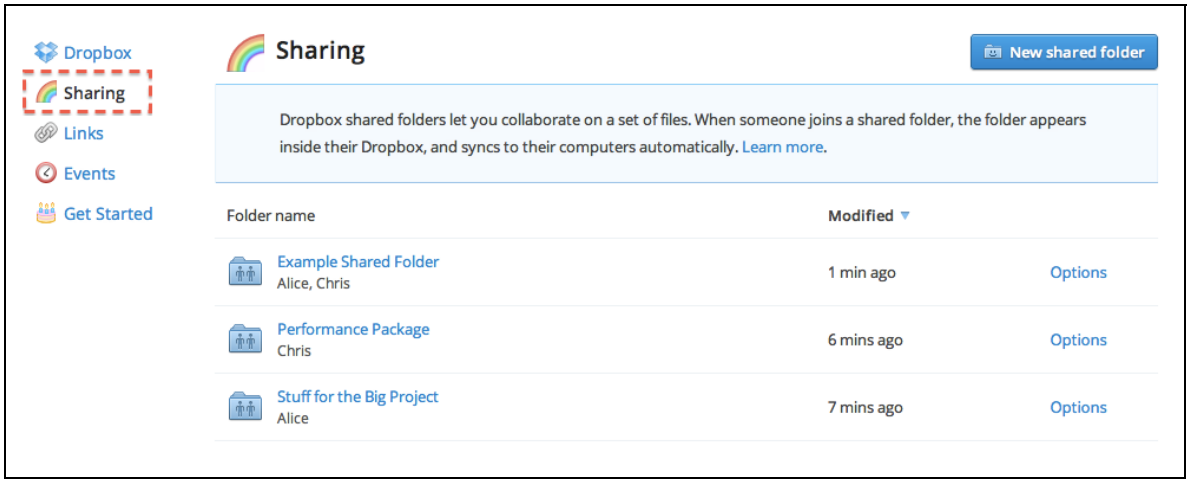

Figure 11. *Sharing* view shows all folders shared with *read-write* access

Further, Dropbox provides visual cues that the files and folders are shared across its interface. A chain linked icon appears next to files and folders where *read-only* access has been granted, and a folder icon overlaid with the outline of two people replaces the standard blank folder icon on a folder that has been shared with *read-write* access. When clicking on a shared folder, the *contextual menu bar* provides a *Shared folder options* button (Figure 12) that displays a list of users with access to the shared folder and provides the ability to e-mail collaborators, revoke their access (*kick out*) or delegate ownership (Figure 13).

Figure 12. *Contextual menu bar* for selected folder that has already been shared

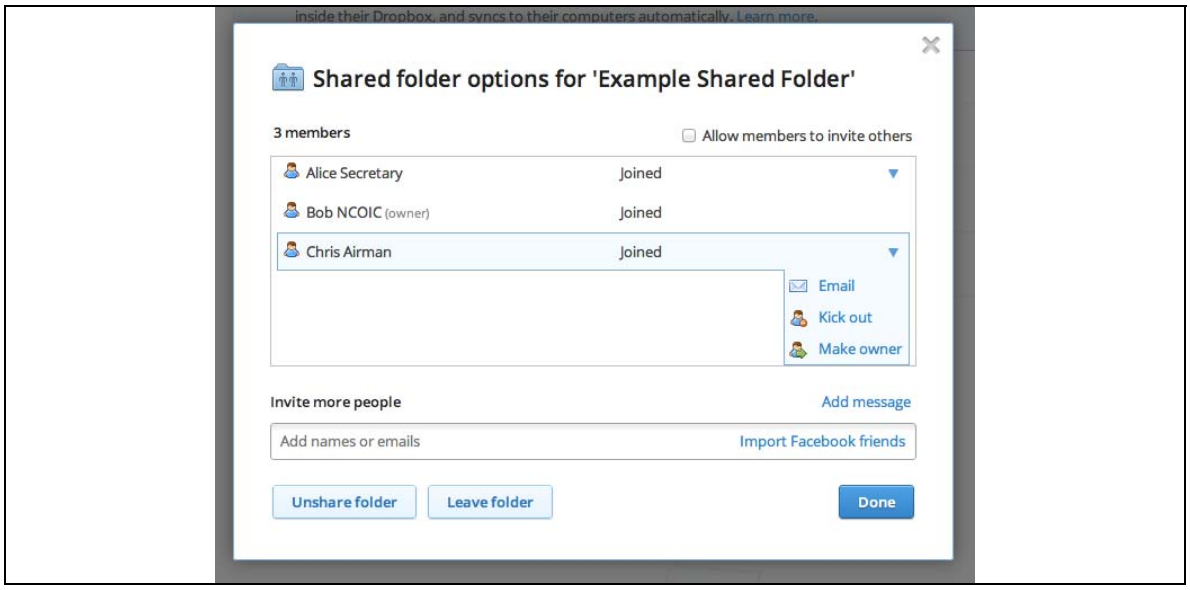

Figure 13. Shared folder options Wizard

In evaluating the usability of this task, we assume the personas have learned the distinctions between Dropbox's *read-only* and *read-write* access permissions before attempting the task. The following sections detail the interactions of each of our personas while accomplishing this task:

a. Alice, the Inexperienced Commander's Secretary

Alice will initially have a difficult time with this task because of the way Dropbox separates the ability to see what she is sharing via the two permission modes into different views. This requires Alice to think about how she has shared a file or folder in the first place (e.g., with *read-only* or *read-write* access). The inconsistent terms used also add to her cognitive friction. For example, all files that were shared using the *Get link* button will show up on the *Links* view, which maps well to Alice's intuition. But all folders shared using the *Invite to folder* button show up on the *Sharing* view. Additionally, having two separate views to see her shared files will initially lead to friction, as she must search across two views to find the file or folder she has shared. It is easy for her to switch views, thought, if she does not find the information she is looking for. These difficulties are minor for Alice and she can easily learn the distinctions through minimal trial-and-error. The concise descriptions at the top of each view help Alice become more familiar with the distinctions between the two views as well as how Dropbox implements *read-only* and *read-write* permissions differently. This aids her learnability of this task.

The fact that the *Links* view does not mimic the *Sharing* view in providing a list of users each file or folder has been shared with causes Alice additional frustration. This is, of course, because Dropbox does not restrict view access to the individuals that received the e-mail; anyone with a link to a file or folder with *read-only* access can see it. But this distinction is not apparent in the view, and will cause Alice frustration since she cannot see whom she has sent the links to. Alice can learn this task with minimal difficulty, and the usability of the tools, once learned, is very simple and allows her to repeat the task with ease.

b. Bob, the Seasoned NCOIC

Like Alice, the inconsistent labels placed on the buttons to share a file or folder, and the buttons to see which file or folder has been shared, will be a source of initial confusion for Bob. However, since the icons for the coinciding buttons are consistent (though the labels are not), Bob will easily be able to follow the consistency of the icons (rather than the inconsistent labels) to determine which method of sharing corresponds with which view. He enjoys the usability provided by the views, which allows him to see all shared files in a single view. No other file sharing solutions he has worked with over his career incorporate such a single view, and trying to figure out what he is personally sharing has historically been a time-consuming chore.

The lack of ability to see with whom a *read-only* link has been shared will also cause Bob initial confusion and frustration, as it is not apparent why this is not possible. As the interface does not explain this shortcoming, Bob will end up using shared folders more often, since they provide the visibility he needs while sharing files.

c. Chris, the Tech-Savvy Young Airman

Chris, who is familiar with trying new user interfaces, will easily learn the methods for accomplishing this task through minimal trial-and-error. The inconsistent terms used for labeling the buttons will not be a problem for him, since the button icons correspond to other similar tasks. Finding the proper views for his needs, and using them, will be simple for him. He will be a slightly frustrated that he cannot see with whom he has shared a *read-only* link, but will accept this as a limitation of the service.

3. Task 5: Audit Collaborators' Actions on a File

This task evaluates the availability, visibility, and usability of auditing tools by requiring the persona to determine who has made changes to a shared file. Since Dropbox only allows collaboration on files within shared folders, this task will be

adjusted to audit the changes on a file within a shared folder. Dropbox provides two methods to accomplish this task; either by reviewing a file's revision history, or through the use of the *Events* view.

Dropbox automatically saves each version of a file and provides the revision history by clicking on the *Previous versions* button under the *More* button in the *contextual menu bar* (Figure 7). The resulting page (Figure 14) lists all previous versions of the file, attributes each version to the collaborator who made the change, and displays when the change was made. The user can also restore a previous version of a file from this page.

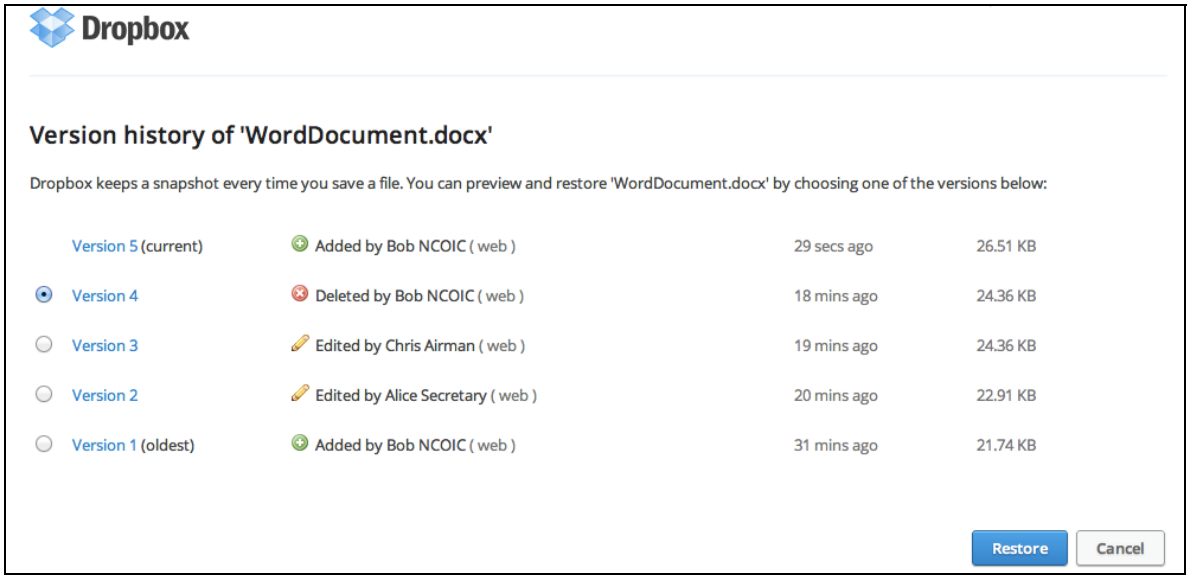

Figure 14. File version history view

The *Events* view lists all changes made across all files within a Dropbox hierarchy, and attributes the change to the respective collaborator. The *Events* view is accessed by clicking the *Events* button in the *left menu bar* of the main interface (Figure 15). A folder dropdown tool in the menu bar of this view provides the ability to filter the changes by a particular shared folder. A calendar dropdown tool allows filtering the results by a particular day.

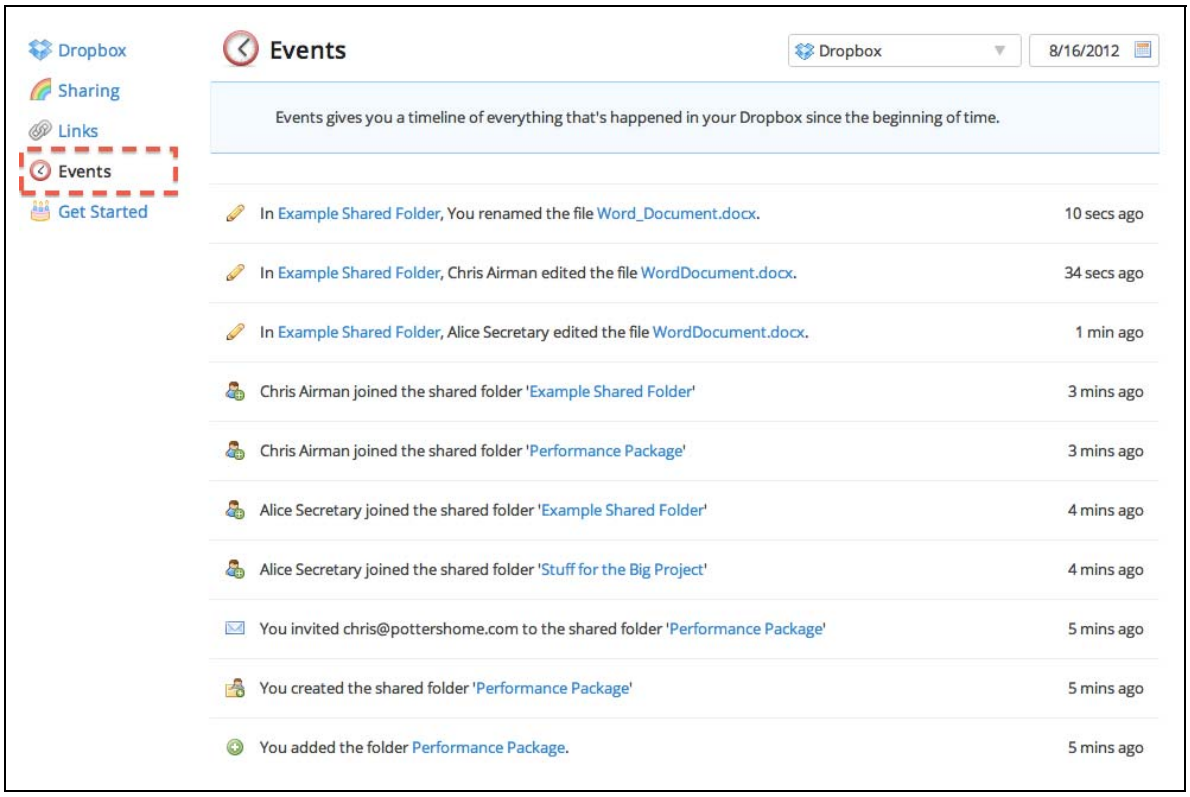

Figure 15. *Events* view lists all the changes made across all files and folders

The following sections detail the interactions of each of our personas while accomplishing this task:

a. Alice, the Inexperienced Commander's Secretary

Alice will not be able to accomplish this task using the *Previous versions* method for a two reasons. First, Alice's intuition would not naturally tell her that the required steps to complete this task are found under a file's revision history. Second, the *Previous versions* button is not only hidden within the *contextual menu bar* and only visible when a file is selected, but also is hidden under the *More* button of the contextual menu bar. Alice will search the interface for a tool that relates to this task, but will not be able to find one.

After some searching, Alice may come across the *Events* button. The word *Events* does not intuitively relate to the task for Alice, but the concise description

found at the top of the view explains that this view provides the information she is looking for. This view is easy to find, simple in its presentation of information, and provides the information Alice needs to see exactly what has been changed across all her files recently. While the first method to accomplish this task would be extremely difficult to learn, the *Events* view is easy to find and presents the required information in a simple, unified page. This view provides easy learnability and high usability for her.

b. Bob, the Seasoned NCOIC

Bob understands that he should be looking for the revision history for a file to complete this task, but, like Alice, he will have significant difficulty finding what he needs buried under the *More* button. He will easily find, however, the *Events* view, and will be pleased to see that it provides the information he needs on one consolidated page. He must visit the page a few times, since the name *Events* was not an intuitive match for him to relate to this task, and, like many IT users, he does not read sentence length text on a page unless required (Krug, 2006). After minor trial-and-error, and finally reading the page description, he is able to use the information provided by the page to accomplish the task.

c. Chris, the Tech-savvy Young Airman

Chris will find the *Previous versions button* with moderate ease through his skills and experience exploring user interfaces. Unlike Bob and Alice, he immediately tries the *More* button to see what other functionality is available through the service. The presentation of previous versions that results is simple and clear enough for him to understand.

Chris will also quickly find the *Events* page as he explores the new user interface. Like Bob, he does not read much of the text description for the page, so it takes him a couple visits to correctly identify the purpose of the page for accomplishing the task. Chris finds both methods of auditing changes done to a file relatively easy to learn and quick to use. In particular, he likes the granularity the filters on the *Events* view provide for narrowing his search.

D. FINDINGS

As the heuristics evaluation and cognitive walkthroughs are conducted, notes should be taken on findings relevant to the organization for consideration of results not immediately apparent. This section presents a sample of the findings of this example evaluation, as well as a summary of the results from the cognitive walkthrough.

1. Good Usability and Security Findings

- Google Drive and Box both provide Single Sign-On capabilities with the incorporation of Security Assertion Markup Language (SAML)-based APIs that integrate with an organization's existing means of authentication. Single Sign-On can be integrated with current PKI certificates for use within the DoD.
- While all three technologies provided some level of notifying data owners and collaborators of changes made to documents, Box allows far more granular control of these notifications. This granularity allows users to immediately see if someone downloaded, uploaded, commented on, previewed, or deleted something from folders they owned, or folders they are sharing and to switch each type of notification on or off as needed.
- Google Drive and Box provides robust tools for an administrator to manage a user's settings and activity within the enterprise.
- Box provides mechanisms to further restrict shared folder access by setting a password on the folder and an expiration date for when the folder access will automatically be revoked.
- Box and Google Drive allow collaborators to make comments on files to enhance collaboration.
- Dropbox provides a LAN sync feature that allows file synchronization to occur locally between devices within the same LAN without requiring the file to traverse the Internet to the cloud servers, thus avoiding bandwidth and latency issues.
- Box reports to have been issued an SSAE 16 type II report certifying they maintain high security practices for storing and handling user's data.
- Google reports their Google Apps for Government offering (which includes Google Drive) has received an authority to operate at the FISMA-Moderate level with a Low operational risk level (Google, 2012b).
- Though none of the solutions have a current FedRAMP security authorization, Box is reportedly pursuing this certification.

2. Bad Usability and Security Findings

- Box offers many additional sharing and collaboration features over Box and Google Drive, but this added functionality tends to increase the cognitive friction and reduce the usability of the product.
- Box and Dropbox save each upload as a new version to avoid inconsistencies. In highly collaborative environments, this means that if two users make changes and save different versions of the same file at the same time, two versions of the file will be created. All the data will be saved, but the collaborators will have to manually merge the inconsistencies between the two files. Google Drive allows users to work on the same document simultaneously, so inconsistencies are very rare.
- Box, by default, automatically provides *read-only* access to any folder and file added to the service. Anyone with a link will be able to access it without the owner explicitly sharing it. This default setting can be changed within the settings.
- Each service stores deleted files in a trash location for users to recover. If deleted from this trash location, Dropbox and Google Drive delete the file permanently (may take time to propagate through their servers) while Box makes the file recoverable for 30 more days before it becomes unrecoverable.
- Google Drive's office productivity suite is only available online. If using these proprietary document file types to allow for synchronous file editing, they will not be accessible when a connection to the Internet is unavailable. The only current exception is by installing a plugin for the Chrome browser. Offline access to Google Drive documents is not available on any other browser.
- Google Drive provides rich automatic versioning features for its proprietary document types only. Other document types common within the DoD (e.g., .pdf, .doc, .xls) are uploaded as completely separate documents and retain no version history.
- When sharing files or folders, all the services default to grant full access rights to collaborators. If less permission is desired, the user needs to explicitly change the default. No warning messages are given to warn that full access is being granted.
- Dropbox keeps a cache of previously used e-mail addresses for collaborators to provide "auto-fill" capabilities when sharing with frequent collaborators. However, Dropbox does not provide a means of clearing this cache of e-mail address

3. Cognitive Walkthrough Findings

The learnability of Dropbox's interface is hindered by the way it differentiates between *read-only* and *read-write* access modes. Cognitive friction would affect all our personas, as they wrestled with understanding these distinctions. While the distinctions are easy enough to understand once explained, they are not apparent when using the interface. Dropbox provides a video tutorial that provides a basic overview of the service but does not walkthrough any of the user interfaces. To find additional written and video tutorials explaining the distinctions between how Dropbox implements *read-only* and *read-write* access modes, one must search through a hierarchy of links under the *Help* menu. Alice had the most difficult challenges figuring out how to implement the security-related tasks. Bob was able to figure these out on his own, but the initial frustration made him weary of sharing files since he was not completely sure if he was sharing them appropriately. Chris suffered the least frustration, as he was able to grasp the new conventions quickly through good trial-and-error skills, and by his familiarity with similar systems and tools.

Dropbox also uses inconsistent labels on its tools for sharing files and folder, and for auditing which files/folders are being shared, which added to the cognitive friction associated with using the tools. This friction decreased the learnability for the security-relevant tools within Dropbox. To ensure users are effectively using the service, a short tutorial should be provided to explain the unique access control conventions Dropbox uses in order to increase learnability, and the reliability that the security-related tools will be used appropriately. Some tasks can be learned through trial-and-error, but users like Alice and Bob may require so much that frustration leads them to use the tools insecurely (provide *read-only* access to everything) or resort to less secure technology, such as e-mail or USB drives.

Once these few initially difficult concepts were understood, the tools provided by Dropbox were found to be highly usable. All tasks required very few steps, tools were consistently placed across the site and easy to find and use, and the appearance of the site was familiar to users and presented minimal distractions. On average, Bob and Alice

found it only moderately difficult (Chris found it easy) to initially locate the tools required to accomplish tasks. However, once found, the consistent and simple interface made it very easy for all the personas to repeat tasks successfully. Dropbox increased user confidence through immediate and simple feedback following most user actions, and decreased user error by providing the ability to easily *undo* most of those actions. The views provided to see what files and folders users have shared, as well as audit who has modified shared files within a single view, saved users time and increased their security awareness. Overall, after a short and marginally difficult learning period, Dropbox's functionality and user interface could provide a robust, simple solution for DoD users to share files in a usably secure manner.

VI. CONCLUSION AND FUTURE WORK

A. CONCLUSION

Success in today's information-dependent society hinges on the ability for members of an organization to share information. With regard to security, this involves both the need to share information files with co-workers, as well as to restrict access to the information from those who do not need it. Cyber threats from both inside and outside the organization seek to circumvent security measures resulting in the exploitation of valuable information.

The majority of research done to better understand the nature of cyber threats has focused on outside attackers and malicious insiders. Far less research has been dedicated to non-malicious insiders, and overlooking this threat can be a great risk to the organization. Many organizations, including the DoD, may downplay this non-malicious insider threat thinking that the impact is insignificant. This thesis has used historical analyses and other research to show that the non-malicious insider threat leads to far more organizational data breaches than malicious insiders and is even more prevalent than the threat from outside attackers, particularly in the government sector (Cisco, 2008; Lynch, 2006; Open Security Foundation, 2011; Privacy Rights Clearinghouse, 2011). Even if leaked data is not intercepted and exploited by an outside enemy, the indirect costs associated with cleaning-up after non-malicious insider data breaches, including the time, money, and resources required to administratively sanitize computers and networks after a breach, contacting leaked PII victims and providing remediation, as well as the loss of public reputation once a leak is reported, can be high.

This thesis started with the premise that the poor usability of existing file sharing systems contributes to the non-malicious insiders inadvertently compromise information. Additionally, when the security features of an IT system are too difficult to use, well-intentioned users often choose to circumvent them. Providing *usability* and maintaining

security in IT systems have traditionally been viewed as conflicting goals. HCI-SEC research has focused on properly aligning both usability and security to achieve truly secure system (Garfinkel, 2005).

Sharing files is a daily task for IT users within highly collaborative organizations like the DoD. Users must collaborate with co-workers, and even share files with themselves for later access from a different location. While numerous options are available within the DoD for sharing files (i.e., e-mail, shared folders), these legacy systems are either not secure, not usable, or neither secure nor usable. This lack of usable security exacerbates the non-malicious insider threat to DoD information systems. As a consequence, unintended data breaches resulting from this threat degrade the security posture of DoD networks. This thesis has described the emergence of cloud-based file sharing technologies, and how they provide numerous usability benefits to IT users while promising highly secure environments. These benefits include global and ubiquitous access to files from any location or computing platform with Internet access, local syncing of files for access during connectivity loss, automatic off-site storage and backup, automatic version control, and simple access control restrictions.

In 2010, the federal government mandated a "Cloud-first" shift in its IT management "using commercial cloud technologies where feasible" (Kundra, 2010, p. 7). Additionally, the National Security Telecommunications Advisory Committee (NSTAC) has advised the President of the United States that cloud-based file sharing capabilities, including *Document Collaboration*, *Project Coordination*, and *Data Archiving and Storage*, are "mission functions which appear most attractive for cloud migration" and "should be considered for earliest programmatic action" (2012, p. 45). To make this strategy a reality, the federal government has implemented security assessments processes, like FedRAMP, to assess the security practices of a CSP and authorize their technology for official use. While these assessments certify the security practices of a CSP's back-end data storage and handling, they do not evaluate the usability an end-user will expect to find while using the CSP's service.

This thesis develops a methodology that organizations, like the DoD, can use to evaluate the usability and security of cloud-based file sharing services from the end-user

perspective. This methodology adapts and combines the concepts of heuristics evaluation (Nielson, 2005a) and cognitive walkthrough (Wharton et al. 1994). The heuristics evaluation assesses whether a cloud-based file sharing technology implements critical usability and security principles, and the cognitive walkthrough determines how usably the technology implements these features.

The heuristics used for this evaluation are based on the recommendations of numerous researchers from the HCI and HCI-SEC communities, and are specifically tailored for the usability and security of cloud-based file sharing systems. Questions are derived from each heuristic to objectively evaluate if the technology implements the principles of a heuristic. As no solution provides the perfect balance of usability and security, the results from this evaluation allow organizational decision makers to determine the appropriate tradeoffs between the competing goals for their organization, and narrow the list of alternatives to those which provide the best balance of security and usability principles.

The cognitive walkthroughs employ the use of personas (Cooper, 2004) and tasks (Wharton et al., 1994) to evaluate the learnability and ultimate usability of a cloud-based file sharing technology's interface. Three personas were defined to represent a range of IT users within the DoD. Ten tasks were defined to represent the tasks DoD users likely to perform a daily basis.

Finally, this thesis has demonstrated the use of our methodology through an evaluation of three popular cloud-based file sharing technologies: Dropbox, Google Drive, and Box. The heuristics evaluation helped determine that Dropbox provided the best implementation of usability and security for our demonstration and, therefore, warranted further evaluation by cognitive walkthrough. The cognitive walkthrough determined that Dropbox's security features are initially difficult to learn, but very usable once learned. Learnability was hindered by the use of an unconventional method for applying *read-only* and *read-write* access modes through completely separate workflows, using inconsistent terms to label corresponding functions, and hiding relevant features from the user. It was determined that these learnability issues could be resolved with minimal training. Once learned, Dropbox displayed excellent usability qualities,

including a minimalist appearance, consistent placement of tools, consolidated auditing of important file sharing activity, immediate feedback following users' actions, and the ability to easily undo most user actions. Through a demonstration of the usability of its end-user interface, Dropbox is recommended as an exceptional solution for providing robust yet simple file sharing functionality to DoD users.

Providing a highly usable tool to share files securely is vitally important to reduce the non-malicious insider's motivation to circumvent an organizations security measures. The methodologies of this thesis have been developed with the DoD in mind; however, as the act of file sharing is common in highly collaborative corporate environments, the methodologies can appeal to many organizations seeking a solution for cloud-based file sharing. The heuristics evaluation provides simple yet critical visibility into whether competing technologies implement important usability and security principles, tailored specifically for cloud-base file sharing systems. The cognitive walkthrough complements the heuristics evaluation and provides valuable insight into how usable a technology will ultimately be for an organization's users.

B. POSSIBLE FUTURE WORK

1. Formal Heuristics Analysis

Using the heuristics developed in this thesis, valuable insight can be gained in a future study that formally analyzes the heuristics (including the questions that have been derived from them) in real-world situations to validate whether they provide the claimed results of better usability and security for the end-user.

2. User Study

This thesis used personas for the cognitive walkthrough demonstration. There are a number of benefits in UI design for using personas rather actual users (Calabria, 2004; Cooper, 2004). However, a field study of actual user interactions with the UI will help provide valuable insight into the usability of the security features of cloud-based file sharing technologies and validate the claims of this thesis for real-world use.

3. DoD-Specific Study

The demonstration used in this thesis provides only an example evaluation using popular cloud-based alternatives and the IFs of a typical DoD organization. As the DoD moves toward a real solution in the cloud, whether through an authorized CSP or developing their own on the DISA cloud, future work could include using the methodology of this thesis in an evaluation that is specifically tailored to actual DoD requirements.

4. Back-end Security Affordances

As this thesis focuses on the front-end usability and security (i.e., the UI affordances for the end user), follow-on research could include expanding the evaluation methodology to consider back-end security affordances like data security, administrator auditing capabilities, and whether the DoD could use commercially available technologies while hosting their own servers to maintain complete control over the information.

5. Additional Technology Evaluations

To demonstrate the methodology, this thesis only evaluated a few of Dropbox's security features. Future work could involve a more comprehensive evaluation of Dropbox, Box, Google Drive, or any other cloud-based file sharing technologies that has relevance for the DoD. Special attention should be paid to systems that would allow the DoD to host its own servers on a private cloud, or to encrypt data on the client, so that DoD data is never made available to the cloud provider. Additionally, the extensive auditing tools provided by Box are very important in a DoD context and should be further evaluated.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM, 42*(12), 40–46. doi:http://doi.acm.org/10.1145/322796.322806

Balfanz, D., Durfee, G., Smetters, D. K., & Grinter, R. E. (2004). In search of usable security: Five lessons from the field. *Security & Privacy, IEEE, 2*(5), 19–24. doi:10.1109/MSP.2004.71

Bauer, L., Cranor, L. F., Reeder, R. W., Reiter, M. K., & Vaniea, K. (2008). A user study of policy creation in a flexible access-control system. Paper presented at the *Proceedings of the Twenty-Sixth Annual SIGCHI Conference on Human Factors in Computing Systems,* Florence, Italy. 543–552. doi:http://doi.acm.org/10.1145/1357054.1357143

Box. (2012). *Collaboration in the cloud.* Retrieved April 6, 2012, from https://www.box.com/about-us

Bradley, T., & PCWorld. (2011). *Pros and cons of bringing your own device to work.* Retrieved from http://www.pcworld.com/businesscenter/article/246760/pros_and_cons_of_bringing_your_own_device_to_work.html

Calabria, T. (2004). *An introduction to personas and how to create them.* Retrieved from http://www.steptwo.com.au/papers/kmc_personas/index.html

Card, S. K., Moran, T. P., & Newell, A. (1983). *The psychology of human-computer interaction*. Hillsdale, NJ: Lawrence Erlbaum Associates.

Cisco. (2008). *Data leakage worldwide: The high cost of insider threats*. San Jose, CA. Retrieved from http://www.cisco.com/en/US/solutions/collateral/ns170/ns896/ns895/white_paper_c11-506224.pdf

Committee on National Security Systems. (2010). *National information assurance (IA) glossary.* (No. CNSSI 4009). Retrieved from www.cnss.gov/Assets/pdf/cnssi_4009.pdf

Computer Emergency Response Team. (May 2008). *Insider threat study.* Retrieved from http://www.cert.org/insider_threat/study.html

Cooper, A. (2004). *The inmates are running the asylum*. Indianapolis, IN: Sams Publishing.

Cranor, L. F., & Garfinkel, S. (2004). Guest editors' introduction: Secure or usable? *Security & Privacy, IEEE, 2 Issue 5*, 16–18. doi:10.1109/MSP.2004.69

Cranor, L. F., & Garfinkel, S. L. (Eds.). (2005). *Security and usability: Designing secure systems that people can use*. Sebastopol, CA: O'Reilly.

Dalal, B., Nelson, L., Smetters, D., Good, N., & Elliot, A. (2008). Ad-hoc guesting: When exceptions are the rule. Paper presented at the *Proceedings of the 1st Conference on Usability, Psychology, and Security,* San Francisco, CA. 9:1-9:5. doi:http://dl.acm.org/citation.cfm?id=1387649.1387658;

Department of Defense. (2003). *Information assurance (IA) implementation.* (DODI 8500.2). Retrieved from http://www.dtic.mil/whs/directives/corres/pdf/850002p.pdf

Department of Defense. (2007a). *Department of defense Information Sharing Strategy*. Retrieved from http://dodcio.defense.gov/Portals/0/Documents/InfoSharingStrategy.pdf

Department of Defense. (2007b). *Information assurance.* (DODD 8500.01E). Retrieved from http://www.dtic.mil/whs/directives/corres/pdf/850001p.pdf

Department of Defense. (2010). *Quadrennial defense review report.* Retrieved from http://www.defense.gov/qdr/images/QDR_as_of_12Feb10_1000.pdf

Department of Defense. (2011). *Department of defense strategy for operating in cyberspace.* (ADA545385). Retrieved from http://www.dtic.mil/docs/citations/ADA545385

Department of Defense. (2012a). *About the department of defense (DOD).* Retrieved from http://www.defense.gov/about/

Department of Defense. (2012b). *Cloud computing strategy*. Retrieved from http://www.defense.gov/news/DoDCloudComputingStrategy.pdf

DeWitt, A. J., & Kuljis, J. (2006). Aligning usability and security: A usability study of polaris. Paper presented at the *Proceedings of the Second Symposium on Usable Privacy and Security,* Pittsburgh, PA. 1–7. doi:http://doi.acm.org/10.1145/1143120.1143122

Dourish, P., & Redmiles, D. (2002). An approach to usable security based on event monitoring and visualization. Paper presented at the *Proceedings of the 2002 Workshop on New Security Paradigms,* Virginia Beach, VA. doi:http://doi.acm.org/10.1145/844102.844116

Dropbox. (2012). *About dropbox.* Retrieved April 4, 2012, from https://www.dropbox.com/about

FedRAMP (2012). *Concept of Operations (CONOPS)*. Retrieved from http://www.gsa.gov/graphics/staffoffices/CONOPS_V1.1_07162012_508.pdf

Garfinkel, S. L. (2005). *Design principles and patterns for computer systems that are simultaneously secure and usable* (Doctoral dissertation). Massachusetts Institute of Technology. Retrieved from http://simson.net/thesis/

Gibson, S. (2011). *Security now* (episode 302). Retrieved from http://www.grc.com/sn/sn-302.htm

Good, N. S., & Krekelberg, A. (2003). Usability and privacy: A study of KaZaA P2P file-sharing. Paper presented at the *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems,* Ft. Lauderdale, FL. doi:10.1145/642611.642636

Google. (2012a). *Google apps for business.* Retrieved May 5, 2012, from https://www.google.com/enterprise/apps/business

Google. (2012b). *Everything your organization needs*. Retrieved Aug 28, 2012 from http://www.google.com/enterprise/apps/government/benefits.html

International Organization for Standardization. (1998). *Guidance on usability.* (ISO 9241-11). Geneva, Switzerland: International Organization for Standardization. Retrieved from www.iso.org/iso/catalogue_detail.htm?csnumber=16883

Ion, I., Sachdeva, N., Kumaraguru, P., & Čapkun, S. (2011). Home is safer than the cloud!: Privacy concerns for consumer cloud storage. Paper presented at the *Proceedings of the Seventh Symposium on Usable Privacy and Security,* Pittsburgh, PA. 13:1–13:20. doi:http://doi.acm.org/10.1145/2078827.2078845

Johnson, M. L., Bellovin, S. M., Reeder, R. W., & Schechter, S. E. (2009). Laissez-faire file sharing: Access control designed for individuals at the endpoints. Paper presented at the *Proceedings of the 2009 Workshop on New Security Paradigms Workshop,* Oxford, United Kingdom. doi:http://doi.acm.org/10.1145/1719030.1719032

Kime, P. (2011). *DoD hit with lawsuit over lost TRICARE data*. ArmyTimes. Retrieved from http://www.armytimes.com/news/2011/10/military-dod-hit-with-lawsuit-over-lost-tricare-data-101311/

Krug, S. (2006). *Don't make me think: A common sense approach to web usability* (2nd ed.). Berkeley, CA: New Riders.

Kundra, V. (2010). *25 point implementation plan to reform federal information technology management.* Retrieved from http://www.cio.gov/documents/25-point-implementation-plan-to-reform-federal%20it.pdf

Lynch, D. M. (2006). Securing against insider attacks. *EDPACS, 34*(1), 10. Retrieved from http://proquest.umi.com/pqdweb?did=1060408421&Fmt=7&clientId=11969&RQT=309&VName=PQD

Lynn, W. F. I. (2010). *Defending a new domain: The pentagon's cyberstrategy.* Retrieved from http://handle.dtic.mil/100.2/ADA527707

Mell, P., & Grance, T. (2011). *The NIST definition of cloud computing.* (NIST SP 800-145). Gaithersburg, MD: National Institute of Standards and Technology. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

Molich, R., & Nielsen, J. (1990). Improving a human-computer dialogue. *Communications of the ACM, 33*(3), 338–348. doi:http://doi.acm.org/10.1145/77481.77486

Morris, R., & Thompson, K. (1979). Password security: A case history. *Communications of the ACM, 22*(11), 594–597. doi:http://doi.acm.org/10.1145/359168.359172

National Security Telecommunications Advisory Committee. (2012). *NSTAC report to the president on cloud computing.* Retrieved from http://www.ncs.gov/nstac/reports/2012-05-15%20NSTAC%20Cloud%20Computing.pdf

Nelson, A. J., Dinolt, G. W., Michael, J. B., & Man-Tak Shing. (2011). A security and usability perspective of cloud file systems. Paper presented at the *2011 6th International Conference on System of Systems Engineering,* Albuquerque, NM. 161–166. doi:10.1109/SYSOSE.2011.5966591

Net Applications. (2012a). *Mobile/tablet operating system market share*. Retrieved August 5, 2012 from http://www.netmarketshare.com/operating-system-market-share.aspx?qprid=8&qpcustomd=1

Net Applications. (2012b). *Desktop operating system market share*. Retrieved August 5, 2012 from http://www.netmarketshare.com/operating-system-market-share.aspx?qprid=8&qpcustomd=0

Nielsen, J. (2005a). *How to conduct a heuristic evaluation.* Retrieved from www.useit.com/papers/heuristic/heuristic_evaluation.html

Nielsen, J. (2005b). *Ten usability heuristics.* Retrieved from www.useit.com/papers/heuristic/heuristic_list.html

Norman, D. A. (2002). *The design of everyday things*. New York, NY: Basic Books.

Norman, D. A. (1983). Design rules based on analyses of human error. *Communications of the ACM, 26*(4), 254–258. doi:http://doi.acm.org/10.1145/2163.358092

Open Security Foundation. (2011). *DataLossDB.* Retrieved March 10, 2011, from http://datalossdb.org/;

Privacy Rights Clearinghouse. (2011). *Chronology of data breaches, security breaches 2005-present.* Retrieved February 18, 2011, from http://www.privacyrights.org/data-breach

Reeder, R. W., & Maxion, R. A. (2005). User interface dependability through goal-error prevention. Paper presented at the *Proceedings of the 2005 International Conference on Dependable Systems and Networks,* Yokohama, Japan. 60–69. doi:http://dx.doi.org/10.1109/DSN.2005.95

Saltzer, J. H., & Schroeder, M. D. (1975). The protection of information in computer systems. *Proceedings of the IEEE, 63*(9), 1278–1308. doi:10.1109/PROC.1975.9939

Schadler, T., Brown, M., & Martyn, H. (2011). *The Forrester wave: Mobile collaboration, Q3 2011*. Cambridge, MA: Forrester Research, Inc.

Smetters, D. K., & Good, N. (2009). How users use access control. Paper presented at the *Proceedings of the 5th Symposium on Usable Privacy and Security,* Mountain View, CA. 15:1–15:12. doi:http://doi.acm.org/10.1145/1572532.1572552

Stewart, T. A. (1997). *Intellectual capital: The new wealth of organizations*. New York, NY: Doubleday.

Stoneburner, G., Gogun, A., & Feringa, A. (2002). *Risk managment guide for information technology systems.* (NIST SP 800-30). Gaithersburg, MD: National Institute of Standards and Technology. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

Swanson, M., Bowen, P., Phillips, A. W., Gallup, D., & Lynes, D. (2010). Contingency planning for federal information systems. (NIST SP 800-34 rev. 1). Gaithersburg, MD: National Institute of Standards and Technology. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf

Symantec. (2009). *Increase in USB-based malware attacks.* Retrieved from http://www.symantec.com/connect/blogs/increase-usb-based-malware-attacks

Takai, T. (2012). *DoD releases mobile device strategy*. Retrieved from http://www.defense.gov/releases/release.aspx?releaseid=15376

U.S. Secret Service, & CERT/SEI. (2008). *Insider threat study; illicit cyber activity in the government sector*. Pittsburgh, PA: Carnegie Mellon University. Retrieved from www.cert.org/archive/pdf/insiderthreat_gov2008.pdf

U.S. Strategic Command Public Affairs. (2010). *Federal times clarification—USB policy.* Retrieved from http://www.stratcom.mil/news/2010/171/Federal_Times_clarification_-_USB_policy;

United States Strategic Command. (December 2011). *U.S. cyber command fact sheets.* Retrieved from http://www.stratcom.mil/factsheets/cyber_command/

Voida, S., Edwards, W. K., Newman, M. W., Grinter, R. E., & Ducheneaut, N. (2006). Share and share alike: Exploring the user interface affordances of file sharing. Paper presented at the *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems,* Montréal, Québec, Canada. 221–230. doi:http://doi.acm.org/10.1145/1124772.1124806

Whalen, T., Smetters, D., & Churchill, E. F. (2006). User experiences with sharing and access control. Paper presented at the *CHI '06 Extended Abstracts on Human Factors in Computing Systems,* Montréal, Québec, Canada. 1517–1522. doi:http://doi.acm.org/10.1145/1125451.1125729

Wharton, C., Rieman, J., Lewis, C., & Polson, P. (1994). Usability inspection methods. In J. Nielsen, & R. L. Mack (Eds.), (pp. 105–140). New York, NY: John Wiley & Sons. Retrieved from http://dl.acm.org/citation.cfm?id=189200.189214

White House, The. (2010). *National security strategy.* Retrieved from http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf

Whitten, A. (2004). *Making security usable.* (PhD, Carnegie Mellon University). Retrieved from www.gaudior.net/alma/MakingSecurityUsable.pdf

Whitten, A., & Tygar, J. D. (1999). Why johnny can't encrypt: A usability evaluation of PGP 5.0. *8th USENIX Security Symposium,* Washington, D.C. 169–184. doi:http://static.usenix.org/events/sec99/whitten.html;

Yee, K. (2002). User interaction design for secure systems. Paper presented at the *Proceedings of the 4th International Conference on Information and Communications Security,* Venice, Italy. doi:http://dl.acm.org/citation.cfm?id=646280.687663

Zipf, G. K. (1949). *Human behavior and the principle of least effort: An introduction to human ecology*. New York, NY: Hafner Publishing.

Zurko, M. E., & Simon, R. T. (1996). User-centered security. Paper presented at the *Proceedings of the 1996 Workshop on New Security Paradigms,* Lake Arrowhead, CA. doi:http://doi.acm.org/10.1145/304851.304859

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Alan Shaffer
   Naval Postgraduate School
   Monterey, California

4. Simson Garfinkel
   Naval Postgraduate School
   Monterey, California

5. William (Joe) Welch
   Naval Postgraduate School
   Monterey, California

6. Dan Boger
   Naval Postgraduate School
   Monterey, California

7. Tom McAndrew
   Coalfire Systems Inc.
   Dallas, Texas